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

(11) EP 4 148 608 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
**15.03.2023 Bulletin 2023/11**

(21) Application number: **22150341.0**

(22) Date of filing: **05.01.2022**

(51) International Patent Classification (IPC):
***G06F 21/71*** $^{(2013.01)}$ ***G06F 21/64*** $^{(2013.01)}$
***H04L 9/32*** $^{(2006.01)}$ ***H04L 9/40*** $^{(2022.01)}$

(52) Cooperative Patent Classification (CPC):
**G06F 21/71; G06F 21/64; H04L 9/3234;**
**H04L 9/3247; H04L 63/0853**

(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**

(30) Priority: **08.09.2021 EP 21195614**

(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) METHODS AND APPARATUS FOR DIGITAL SIGNATURES

(57) The present invention relates to a data processing apparatus (50) comprising a secure portion (52), wherein the secure portion (52) comprises a private key (13), an unencrypted private certificate key (33), and a seed (21) generated based on a private certificate key (33), wherein the private key (13), the unencrypted private certificate key (33), and the seed (21) are non-extractable from the secure portion (52). The present invention also relates to a method, wherein the method uses the data processing apparatus (50) the method comprising: the secure portion (52) receiving a signing request (100); in the secure portion (52), generating a signature (121) signed with a private key derived from the seed (21) and signing the signature (121) with the unencrypted private certificate key (33) and thus generating a signature (133) signed with the unencrypted private certificate key (33); and outputting the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key (33).

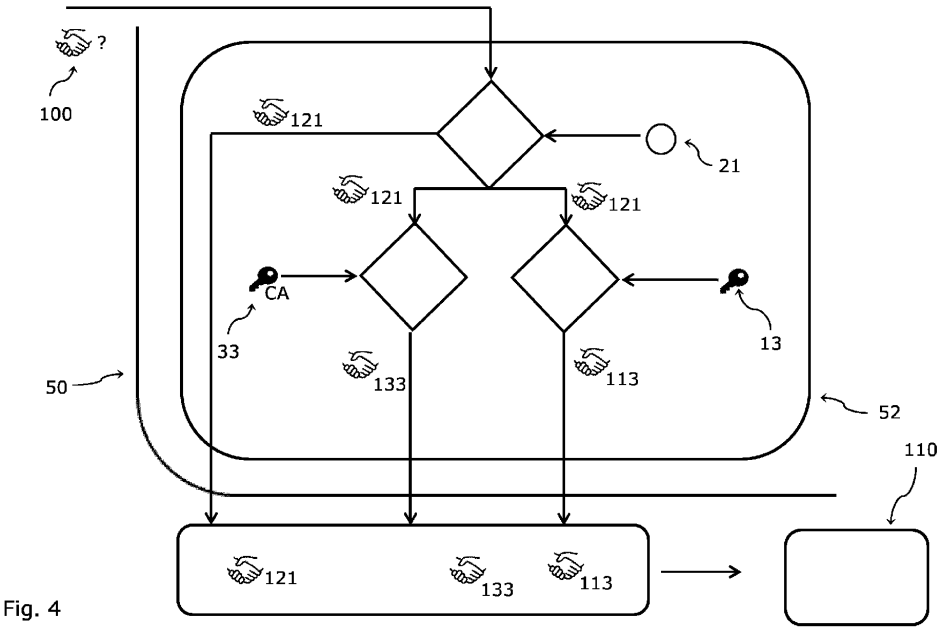

Fig. 4

Processed by Luminess, 75001 PARIS (FR)

## Description

**[0001]** The present invention relates to digital signatures. For examples, digital signature can be used to sign blockchain transactions, smart contracts, or to provide time stamping.

**[0002]** While many methods are known to provide digital signatures, they have certain shortcomings and disadvantages, particularly with regard to traceability, and security against forgery.

**[0003]** The present invention seeks to overcome or at least alleviate the shortcomings and disadvantages of prior art methods. It is therefore an object of the present invention to provide a technology for digital signatures that is improved vis-à-vis the prior art, e.g., with regard to traceability and/or security against forgery.

**[0004]** These objects are met by the present invention.

**[0005]** In a first aspect, the present invention relates to a method. The method comprises providing a data processing apparatus, wherein the data processing apparatus comprises a secure portion, wherein the secure portion comprises a private key that cannot be extracted from the secure portion, wherein the secure portion comprises a public key corresponding to the private key; the data processing apparatus providing a signing request, the public key, and a serial number; based on the signing request, the public key, and the signing request, an external data processing apparatus generating a signed digital certificate; and providing the signed digital certificate to the data processing apparatus. It should be understood that the method according to the first aspect relates to setting up and initializing the data processing apparatus. To differentiate the data processing apparatus pre and post initialization, the data processing apparatus that has not yet been initialized may also be referred to as native or initial data processing apparatus.

**[0006]** The secure portion may comprise a random number generator that cannot be extracted from the secure portion, and the method may comprise the random number generator generating the serial number.

**[0007]** The private key may be generated based on an output from the random number generator.

**[0008]** The data processing apparatus may be a smart card.

**[0009]** The smart card may have near field communication functionality.

**[0010]** The method may comprise providing the signed digital certificate to a data processing system; the data processing system receiving personal user data from a user; providing a public certificate key to the data processing system; the data processing system generating a signed digital system certificate signed with the public certificate key based on the personal user data, the signed digital certificate, and the public certificate key; and providing the signed digital system certificate to the data processing apparatus. It should be understood that providing a public certificate key to the data processing system also encompasses that the public certificate key is generated by the data processing system.

**[0011]** The method may comprise generating the public certificate key and a corresponding private certificate key; encrypting the private certificate key with the public key and thus generating a wrapped key; and providing the wrapped key to the secure portion of the data processing apparatus.

**[0012]** Generating the public certificate key and the corresponding private certificate key, encrypting the private certificate key with the public key to thus generate the wrapped key, and providing the wrapped key to the secure portion of the data processing apparatus may be performed by the data processing system, and wherein the wrapped key is provided from the data processing system to the secure portion of the data processing apparatus.

**[0013]** Generating the public certificate key and the corresponding private certificate key, encrypting the private certificate key with the public key to thus generate the wrapped key, and providing the wrapped key to the secure portion of the data processing apparatus may be performed by a further data processing system; and the method may further comprise providing the public key from the data processing apparatus to the further data processing system; wherein providing the public certificate key to the data processing system comprises providing the public certificate key from the further data processing system to the data processing system.

**[0014]** The method may comprise: in the secure portion, unencrypting the wrapped key with the private key and thus obtaining the private certificate key.

**[0015]** The method may comprise: in the secure portion, generating a seed based on the private certificate key.

**[0016]** By means of the described method, the data processing apparatus may be set up and initialized. It will be understood that after performing the method, the data processing apparatus comprises the signed digital certificate and the signed digital system certificate (signed by the public certificate key). Furthermore, the secure portion of the data processing apparatus then also comprises the seed, the private key and the private certificate key.

**[0017]** In a further aspect, the present invention relates to an initialization method to initialize a data processing apparatus comprising a secure portion, wherein the initialization method comprises: generating a remote asymmetric key pair comprising a remote private key and a remote public key in a remote signature system, providing the remote public key to the secure portion of the data processing apparatus, and generating signing credentials, wherein the remote signature system is configured to sign a data structure when receiving the signing credentials.

**[0018]** The signing credentials may be generated by the remote signature system.

**[0019]** The initialization method may further comprise providing the signing credentials to the data processing apparatus, e.g., to the secure portion of the data processing apparatus.

**[0020]** The present invention also relates to a combined method. The combined method comprises the method as discussed above and the initialization method as discussed above. The data processing apparatus of the method is the data processing apparatus of the initialization method. It will be understood that the secure portion of the method is the secure portion of the initialization method.

**[0021]** In another aspect, the present invention relates to a data processing apparatus comprising a secure portion; wherein the secure portion comprises a private key, an unencrypted private certificate key, and a seed generated based on a private certificate key, wherein the private key, the unencrypted private certificate key, and the seed are non-extractable from the secure portion.

**[0022]** Such a data processing apparatus, e.g., the data processing apparatus obtained by the method according to the first aspects, may have improved functionality.

**[0023]** In particular, by means of the seed, and the private certificate key, the data processing apparatus may sign signatures, e.g., signatures of transactions that can then be output, e.g., broadcasted.

**[0024]** For example, by using the unencrypted private certificate key, which may be provided by an external entity, additional validation may be provided. For example, the private certificate key may be issued by a recognized entity, and a further user may only recognize a signature if a key issued by such an entity is used, thereby providing a white listing functionality.

**[0025]** The data processing apparatus may comprise a signed digital certificate.

**[0026]** The secure portion comprises may be random number generator.

**[0027]** The data processing apparatus may be a smart card.

**[0028]** The smart card may have near field communication functionality.

**[0029]** The data processing apparatus may comprise a serial number generated by the random number generator.

**[0030]** The data processing apparatus may comprise a signed digital system certificate, wherein the signed digital system certificate is signed with a public certificate key corresponding to the private certificate key, and wherein the signed digital system certificate is based on personal user data, the signed digital certificate and the public certificate key.

**[0031]** As the data processing apparatus may comprise the signed digital certificate and/or the signed digital system certificate, any of these certificates can also be appended to a signature of a transaction, such that the present technology also enables the user of the data processing apparatus to provide identification basis if needed or desired.

**[0032]** The data processing apparatus may be obtainable, and may preferably be obtained, by the method as discussed before.

**[0033]** The described technology and particularly the described method to initialize the data processing apparatus also allows a data processing apparatus with corresponding functionality to be generated, e.g., in case the data processing apparatus is lost. In particular, the private certificate key can again be wrapped and provided to another data processing apparatus in the same manner (i.e., wrapped by a public key), and unencrypted in the same manner. Thus, also another data processing apparatus can be provided with the unencrypted private certificate key and the seed derived from the unencrypted private certificate key to thus provide corresponding functionality to another data processing apparatus, e.g., in case of loss of a data processing apparatus. Corresponding considerations also apply to the digital system certificate, which can also be provided with mostly corresponding data in case a new identification of a user is provided. Overall, embodiments of the present technology therefore also allow the implementation of backup solutions.

**[0034]** It will also be understood that the described technology allows for revocations of the described certificates. That is, e.g., in case a data processing apparatus is lost, the external entities which generated one of the certificates, can revoke the corresponding certificate to thereby increase security of the data processing apparatus.

**[0035]** It will be understood that in some instances, at least one of the certificates of the data processing apparatus may also be output together with signed signatures. This allows to check whether the certificates are still valid.

**[0036]** Furthermore, as discussed, the unencrypted private certificate key is only present in the secure portion of the data processing apparatus and cannot be extracted from it. Thus, the respective data processing apparatus can also not be forged by a user.

**[0037]** The data processing apparatus may be configured to only allow data structures signed by a key derived from seed to be signed by the unencrypted private certificate key.

**[0038]** The data processing apparatus may be configured to only allow data structures signed by a key derived from seed to be signed by the private key.

**[0039]** The present invention also relates to a data processing apparatus, wherein the data processing apparatus comprises a secure portion, wherein the secure portion comprises a remote public key.

**[0040]** The data processing apparatus may be initialized by the initialization method discussed above.

**[0041]** In all aspects, the secure portion may comprise a remote public key.

**[0042]** The data processing apparatus may be obtained by the combined method discussed above.

**[0043]** The remote public key may correspond to a remote private key stored in a remote signature system.

**[0044]** The data processing apparatus may further comprise signing credentials to trigger a signature by the remote signature system.

**[0045]** In a still further aspect, the present invention relates to a method, wherein the method uses the data processing apparatus according to any of the preceding apparatus embodiments, the method comprising

the secure portion receiving a signing request,
in the secure portion, generating at least one signature, and
outputting the at least one signature.

**[0046]** The method may us the data processing apparatus discussed above. Generating at least one signature may comprise generating a signature signed with a private key derived from the seed and signing the signature with the unencrypted private certificate key and thus generating a signature signed with the unencrypted private certificate key, and outputting the at least one signature may comprise outputting the signature signed with the private key derived from the seed and the signature signed with the unencrypted private certificate key.

**[0047]** The method may further comprise: in the secure portion, signing the signature with the private key and thus generating a signature signed with the private key; and outputting the signature signed with the private key together with the signature signed with the private key derived from the seed and the signature signed with the unencrypted private certificate key.

**[0048]** The method may use the data processing apparatus discussed before, and the method may further comprise outputting the signed digital certificate together with the signature signed with the private key derived from the seed and the signature signed with the unencrypted private certificate key.

**[0049]** The method may use the data processing apparatus as discussed before, and the method may further comprise outputting the signed digital system certificate together with the signature signed with the private key derived from the seed and the signature signed with the unencrypted private certificate key.

**[0050]** The method may further comprises: a remote signature system receiving the signing request, the remote signature system signing the signing request with a remote private key corresponding to the remote public key and thus generating a pre-signature, the secure portion receiving the pre-signature, and in the secure portion verifying with the remote public key that the pre-signature is the signing request signed with the remote private key, wherein generating the at least one signature in the secure portion and outputting the at least one signature depend on the successful verification with the remote public key that the pre-signature is the signing request signed with the remote private key.

**[0051]** The method may further comprises the remote signature system receiving signing credentials, wherein the remote signature system signing the signing request with a remote private key corresponding to the remote public key and thus generating a pre-signature may depend on the remote signature system receiving the signing credentials.

**[0052]** The method may further comprise disabling a capability of the remote signature system to sign with the remote private key.

**[0053]** By using this technology, the signature functionality of the data processing apparatus is linked to the remote signature system, which may be, cloud based. In particular, the signature functionality of the data processing apparatus, e.g., a smart card, depends on the data processing apparatus receiving the pre-signature, i.e., the signing request signed with the remote private key of the remote signature system. Only when the pre-signature signed by the remote signature system is received by the data processing apparatus, will the data processing apparatus sign the signing request.

**[0054]** This allows the signing functionality of the data processing apparatus to be controlled by the signing functionality of the remote signature system. For example, in case the data processing apparatus is lost, the respective remote private key in the remote signature system can be blocked, thereby blocking the signing functionality of the data processing apparatus, which may increase security against fraud, e.g., in case the data processing apparatus is stolen.

**[0055]** The present invention is also defined by the following numbered embodiments.

**[0056]** 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, those embodiments are meant.

M1. A method comprising

providing a data processing apparatus (50), wherein the data processing apparatus (50) comprises a secure portion (52), wherein the secure portion (52) comprises a private key (13) that cannot be extracted from the secure portion (52), wherein the secure portion (52) comprises a public key (14) corresponding to the private key (13),
the data processing apparatus providing a signing request (15), the public key (14), and a serial number (12),
based on the signing request (15), the public key (14), and the signing request (15), an external data processing apparatus (60) generating a signed digital certificate (16), and
providing the signed digital certificate (16) to the data processing apparatus (50).

M2. The method according to the preceding embodiment, wherein the secure portion (11) comprises a random number generator (11) that cannot be extracted from the secure portion (52), wherein the method comprises the random number generator (11) generating the serial number (12).

M3. The method according to the preceding embodiment, wherein the private key (13) is generated based on an output from the random number generator (11).

M4. The method according to any of the preceding embodiments, wherein the data processing apparatus (50) is a smart card.

M5. The method according to the preceding embodiment, wherein the smart card has near field communication functionality.

M6. The method according to any of the preceding embodiments, wherein the method comprises

providing the signed digital certificate (16) to a data processing system (70),
the data processing system (70) receiving personal user data (82) from a user (80), providing a public certificate key (34) to the data processing system (70),
the data processing system (70) generating a signed digital system certificate (36) signed with the public certificate key (34) based on the personal user data (82), the signed digital certificate (16), and the public certificate key (34),
providing the signed digital system certificate (36) to the data processing apparatus (50).

M7. The method according to the preceding embodiment, wherein the method comprises

generating the public certificate key (34) and a corresponding private certificate key (33),
encrypting the private certificate key (33) with the public key (14) and thus generating a wrapped key (40), and providing the wrapped key (40) to the secure portion (52) of the data processing apparatus.

M8. The method according to the preceding embodiment, wherein
generating the public certificate key (34) and the corresponding private certificate key (33), encrypting the private certificate key (33) with the public key (14) to thus generate the wrapped key (40), and providing the wrapped key (40) to the secure portion (52) of the data processing apparatus are performed by the data processing system (70), and wherein the wrapped key (40) is provided from the data processing system (70) to the secure portion (52) of the data processing apparatus (50). [Fig. 2a]

M9. The method according to the penultimate embodiment, wherein

generating the public certificate key (34) and the corresponding private certificate key (33), encrypting the private certificate key (33) with the public key (14) to thus generate the wrapped key (40), and providing the wrapped key (40) to the secure portion (52) of the data processing apparatus are performed by a further data processing system (72),
wherein the method further comprises providing the public key (14) from the data processing apparatus (50) to the further data processing system (72),
wherein providing the public certificate key (34) to the data processing system (70) comprises providing the public certificate key (34) from the further data processing system (72) to the data processing system (70). [Fig. 2b]

M10. The method according to any of the 3 preceding embodiments, wherein the method comprises
in the secure portion (52), unencrypting the wrapped key (40) with the private key (13) and thus obtaining the private certificate key (33).

M11. The method according to the preceding embodiment, wherein the method comprises
in the secure portion (52), generating a seed (21) based on the private certificate key (33).

**[0057]** Below, initialization embodiments will be discussed. These embodiments are abbreviated by the letter I followed by a number. Whenever reference is herein made to initialization embodiments, those embodiments are meant.

I1. An initialization method to initialize a data processing apparatus (50) comprising a secure portion (52), wherein the initialization method comprises

generating a remote asymmetric key pair (200, 202) comprising a remote private key (200) and a remote public key (202) in a remote signature system (20),
providing the remote public key (202) to the secure portion (52) of the data processing apparatus, and
generating signing credentials (220), wherein the remote signature system (20) is configured to sign a data structure when receiving the signing credentials (220).

12. The initialization method according to the preceding embodiment, wherein the signing credentials (220) are generated by the remote signature system (20).

13. The initialization method according to any of the 2 preceding embodiments, further comprising providing the signing credentials (220) to the data processing apparatus (50), e.g., to the secure portion (52) of the data processing apparatus (50).

C1. A combined method, wherein the combined method comprises the method according to any of the preceding method embodiments and the initialization method according to any of the preceding initialization embodiments, wherein the data processing apparatus (50) of the method is the data processing apparatus (50) of the initialization method.

**[0058]** It will be understood that the secure portion of the method is the secure portion of the initialization method.

**[0059]** Below, apparatus embodiments will be discussed. These embodiments are abbreviated by the letter A followed by a number. Whenever reference is herein made to apparatus embodiments, these embodiments are meant.

A1. A data processing apparatus (50) comprising a secure portion (52),

wherein the secure portion (52) comprises

a private key (13),
an unencrypted private certificate key (33), and
a seed (21) generated based on a private certificate key (33),

wherein the private key (13), the unencrypted private certificate key (33), and the seed (21) are non-extractable from the secure portion (52).

A2. The data processing apparatus (50) according to the preceding embodiment, wherein the data processing apparatus (50) comprises a signed digital certificate (16).

A3. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the secure portion (52) comprises a random number generator (11).

A4. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the data processing apparatus (50) is a smart card.

A5. The data processing apparatus (50) according to the preceding embodiment, wherein the smart card has near field communication functionality.

A6. The data processing apparatus (50) according to any of the preceding embodiments with the features of embodiment A3, wherein the data processing apparatus comprises a serial number (12) generated by the random number generator (11).

A7. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the data processing apparatus (50) comprises a signed digital system certificate (36), wherein the signed digital system certificate (36) is signed with a public certificate key (34) corresponding to the private certificate key (33), and wherein the signed digital system certificate (36) is based on personal user data (82), the signed digital certificate (16) and the public certificate key (34).

A8. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the data processing apparatus (50) is obtainable, and preferably obtained, by the method according to embodiment M11.

A9. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the data processing apparatus (50) is configured to only allow data structures signed by a key derived from seed (21) to be signed by the unencrypted private certificate key (33).

A10. The data processing apparatus (50) according to any of the preceding apparatus embodiments, wherein the data processing apparatus (50) is configured to only allow data structures signed by a key derived from seed (21) to be signed by the private key (13). A11. A data processing apparatus (50), wherein the data processing apparatus (50) comprises a secure portion (52), wherein the secure portion (52) comprises a remote public key (202).

A12. The data processing apparatus (50) according to the preceding embodiment, wherein the data processing apparatus (50) is initialized by the initialization method according to any of the preceding initialization embodiments.

A13. The data processing apparatus (50) according to any of the embodiments A1 to A10, wherein the secure portion (52) comprises a remote public key (202).

A14. The data processing apparatus (50) according to the preceding embodiment, wherein the data processing apparatus (50) is obtained by the combined method according to embodiment C1.

A15. The data processing apparatus (50) according to any of the 4 preceding embodiments, wherein the remote public key (202) corresponds to a remote private key (200) stored in a remote signature system (20).

A16. The data processing apparatus (50) according to the preceding embodiment, wherein the data processing apparatus (50) further comprises signing credentials (20) to trigger a signature by the remote signature system (20).

N1. A method, wherein the method uses the data processing apparatus (50) according to any of the preceding apparatus embodiments, the method comprising

the secure portion (52) receiving a signing request (100),
in the secure portion (52), generating at least one signature (121, 133, 113, 250), and
outputting the at least one signature (121, 133, 113, 250).

N2. The method according to the preceding embodiment, wherein the method uses the data processing apparatus (50) according to any of the preceding apparatus embodiments with the features of embodiment A1, wherein

generating at least one signature (121, 133, 113, 250) comprises generating a signature (121) signed with a private key derived from the seed (21) and signing the signature (121) with the unencrypted private certificate key (33) and thus generating a signature (133) signed with the unencrypted private certificate key (33), and
outputting the at least one signature (121, 133, 113, 250) comprises outputting the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key (33).

N3. The method according to the preceding embodiment, wherein the method further comprises

in the secure portion (52), signing the signature (121) with the private key (13) and thus generating a signature (113) signed with the private key (13),
outputting the signature (113) signed with the private key (13) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

N4. The method according to any of the 2 preceding embodiments, wherein the method uses the data processing apparatus (50) according to any of the preceding apparatus embodiments with the features of embodiment A2, wherein the method further comprises outputting the signed digital certificate (16) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

N5. The method according to any of the 3 preceding embodiments, wherein the method uses the data processing apparatus (50) according to any of the preceding apparatus embodiments with the features of embodiment A7, wherein the method further comprises outputting the signed digital system certificate (36) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

N6. The method according to any of the 5 preceding embodiments, wherein the method uses the data processing apparatus according to any of the preceding apparatus embodiments with the features of embodiment A11 or A13, wherein the method further comprises

a remote signature system (20) receiving the signing request (100),
the remote signature system (20) signing the signing request (100) with a remote private key (200) corresponding to the remote public key (202) and thus generating a pre-signature (210),
the secure portion (52) receiving the pre-signature (210), and
in the secure portion (52) verifying with the remote public key (202) that the pre-signature (210) is the signing request (100) signed with the remote private key (200),
wherein generating the at least one signature (121, 133, 113, 250) in the secure portion (52) and outputting the at least one signature (121, 133, 113, 250) depend on the successful verification that the pre-signature (210) is the signing request (100) signed with the remote private key (200) with the remote public key (202).

N7. The method according to the preceding embodiment,

wherein the method further comprises the remote signature system (20) receiving signing credentials (220),
wherein the remote signature system (20) signing the signing request (100) with a remote private key (200) corresponding to the remote public key (202) and thus generating a pre-signature (210) depends on the remote signature system (20) receiving the signing credentials (220).

N8. The method according to any of the 2 preceding embodiments,
wherein the method further comprises disabling a capability of the remote signature system (20) to sign with the remote private key (200).

**[0060]** Embodiments of the present technology will now be described with reference to the accompanying drawings, and the embodiments should be understood to explain, but not to limit, the scope of the present technology.

Fig. 1 depicts a setup of a data processing apparatus according to an embodiment of the present technology;
Fig. 2a depicts an initialization of a data processing apparatus according to an embodiment of the present technology;
Fig. 2b depicts another initialization of a data processing apparatus according to another embodiment of the present technology;
Fig. 3 depicts in more detail steps of an initialization of embodiments of the present technology;
Fig. 4 depicts a signing procedure according to embodiments of the present technology;
Fig. 5 depicts a flow chart diagram of a setup of a data processing apparatus corresponding to Fig. 1;
Fig. 6 depicts a flow chart diagram of an initialization of a data processing apparatus corresponding to Figs. 2a or 2b, and 3;
Fig. 7 depicts a flow chart diagram of a signing procedure corresponding to Fig. 5;
Fig. 8 depicts a further initialization of a data processing apparatus according to an embodiments of the present technology (that may be used together with or independently from the initialization of Figs. 2a/2b);
Fig. 9 depicts a signing procedure according to embodiments of the present technology; and
Fig. 10 depicts a further signing procedure according to embodiments of the present technology.

**[0061]** Fig. 1 depicts a data processing apparatus 50 that may be realized as a smart card, e.g., a smart card with near field communication (NFC) functionality. In the following, reference will also be made to smart card 50, but the skilled person will understand that data processing apparatus 50 may also be realized in a different manner than a smart card, independent of whether reference is made to a smart card or a data processing apparatus. Prior to its initialization, the data processing apparatus 50 may also be referred to as original or native data processing apparatus 50.

**[0062]** The data processing apparatus 50 comprises a secure portion 52, which may also be referred to as secure enclave 52. The secure portion 52 can provide hardware and software protection for maintaining the secrecy of data in the secure portion 52. More particularly, the data processing apparatus 50 (e.g., the smart card) can be programmed so that only defined data may leave the secure portion 52, while other data cannot leave the secure portion 52. The secure portion 52 can comprise one or more secure microcontroller and one or more secure memory components.

**[0063]** The secure portion 52 comprises a random number generator 11 (and it should be understood that this term also encompassed a pseudo random number generator).

**[0064]** In a first step S1 (also see Fig. 5), the random number generator 11 generates a random serial number 12. Furthermore, in a step S2, a pair of a private key 13 and a public key 14 is generated in the secure portion 52. The keys 13, 14 are asymmetric cryptographic keys. This may be based on a random number generated by the random number generator 11, and it should be understood that it is not critical whether step S2 is carried out after step S1 or before. The data processing apparatus 50 is configured such that the private key 13 cannot be extracted from the secure portion 52.

**[0065]** In a further step S3, the random serial number 12, the public key 14 and a signing request 15 are provided to an external data processing apparatus 60, and the external data processing apparatus 60 generates and signs a digital certificate 16 in a step S4, e.g., by using a root certificate.

**[0066]** The digital certificate 16 may be an X509 digital certificate and is signed by a root certificate of the external data processing apparatus 60. The digital certificate 16 contains the serial number 12, the public key 14, and may additionally contain information relating to the type of the data processing apparatus 50. The digital certificate 16 may provide functionality relating to on card digital signature and decryption.

**[0067]** In a further step S5, the digital certificate 16 is provided to the data processing apparatus 50. After this step, the data processing apparatus 50 is unique by its serial number 12 and cannot be forged due to the digital certificate 16.

**[0068]** It will be understood that the steps S1 to S5 described in conjunction with Fig. 1 typically relate to a factory setup of the data processing apparatus 50, e.g., smart card 50.

**[0069]** As depicted in Fig. 2a and Fig. 6, in a step T1, an identity of a user 80 may be verified by using a data processing system 70, which may also be referred to as third party certification system 70 or third party certification authority 70. It should be understood that the data processing system 70 typically comprises a processor and a memory to store data. During the identify verification process, the user may provide personal data 82 to the data processing system 70.

**[0070]** In a further step T2, the data processing system 70 generates a pair of a public certificate key 34 and a private certificate key 33. It should be understood that these keys are normal asymmetric cryptographic keys and the specification that these keys are "certificate" keys should merely differentiate them from the keys 13 and 14. It should thus be understood that the certificate keys 33, 34 are different from keys 13, 14.

**[0071]** In a step T3, the public certificate key 34 and the personal user data 82 are provided, and furthermore, the signed digital certificate 16 are provided (the latter one from the data processing apparatus 50), and a certificate signing request 90 is generated based thereon. In the depicted embodiment, this step T3 is performed in the data processing system 70. However, it should be understood that this step T3 may also be performed external to the data processing system 70.

**[0072]** A further step T4 may be performed in the data processing system 70, wherein step T4 may comprise different sub-steps. In a sub-step T4a, the authenticity of the digital certificate 16 may be verified. In a sub-step T4b, a digital certificate 36 signed with the public certificate key 34 may be generated, which will be referred to as digital system certificate 36 (merely to differentiate its terminology from digital certificate 16). The digital system certificate 36 may include the personal user data 82 (e.g., a name of the user, a passport ID of the user, and/or an address of the user), the public certificate key 34, and the signed digital certificate 16. In a sub-step T4c, the private certificate key 33 may be encrypted with the public key 14 to thus generated wrapped (or encrypted) private certificate key 40 (in this regard, it is noted that the public key 14 is contained in the signed digital certificate 16 and thus also in the certificate signing request 90).

**[0073]** In a step T5, the wrapped private certificate key 40 and the digital system certificate 36 are provided to the data processing apparatus 50.

**[0074]** However, while many functionalities were described to be performed by the data processing system 70 in the embodiment depicted in Fig. 2a, it should be understood that this is merely exemplary and that the functionalities and steps may also be performed by different systems. This is exemplarily depicted in Fig. 2b. The functionality of the embodiment depicted in Fig. 2b mostly correspond to the functionality of the embodiment depicted in Fig. 2a. However, the embodiment in Fig. 2b comprises a further data processing system 72 and some of the functionalities are realized in this further data processing system 72, which typically comprises a processor and a memory. The additional data processing system 72 may be, e.g., a hardware security module.

**[0075]** In particular, the further data processing system 72 may generate the pair of the public certificate key 34 and the private certificate key 33 (i.e., step T2, see Fig. 6), and the public certificate key 34 may be provided to the data processing system 70. In the data processing system 70, it is used to generate the certificate signing request 90 (step T3) and to generate the digital system certificate 36 signed with the public certificate key 34 (as previously discussed). Again, this digital certificate key may then be provided to the data processing apparatus 50.

**[0076]** Furthermore, the public key 14 may be provided from the data processing apparatus 50 to the additional data processing system 72 (where it will be understood that the public key 14 may be extracted from the secure portion 52 of the data processing apparatus 50). Further still, in the additional data processing system 72, the private certificate key 33 may be wrapped (i.e., encrypted) with the public key 14 (sub step T4c) to thus generate the wrapped private certificate key 40, which can then be provided to the data processing apparatus (part of step T5).

**[0077]** Fig. 3 depicts an enlarged section of the data processing apparatus 50 to further illustrate additional steps performed after the processing apparatus 50 receives the wrapped certificate key 40. As depicted, the wrapped certificate key 40 is provided to the secure portion 52 of the data processing apparatus 50.

**[0078]** In a step T6 performed in the secure portion 52, the wrapped certificate key 40 is decrypted by means of the private key 13 to thus arrive at the unencrypted private certificate key 33, which cannot be extracted from the secure portion 52. In a step T7 performed in the secure portion 52, based on the unencrypted private certificate key 33, a seed 21 is generated. For example, the seed 21 may be generated from the unencrypted private certificate key 33 via a hard coded secret derivation function inside the secure portion 52 of the data processing apparatus 50. For example, the seed 21 may be a BIP32 seed, and it may be derived by means of a multiple SHA256 and AES encryption algorithm.

**[0079]** Thus, after completion of the step T7, there is a seed 21 in the secure portion 52 of the data processing apparatus 50.

**[0080]** Generally, it will be understood that the steps T1 to T7 may relate to the initialization of the data processing apparatus. By means of the initialization, the data processing apparatus 50 may be equipped with additional functionalities.

**[0081]** For example, the data processing apparatus 50 may be used as discussed in conjunction with Fig. 4 and Fig. 7.

**[0082]** In a step U1, a signing request 100 is provided to the data processing apparatus 50 and more particularly to the secure portion 52 thereof. For example, the signing request 100 may be a signing request 100 relating to a transaction on a blockchain network, or signing request relating to a smart contract.

**[0083]** In a step U2, the respective signing request is fulfilled, i.e., the respective signature 121 for the request is generated. The signature 121 is generated based on the signing request 100 and a private key derived from the seed 21, and it should be understood that both the seed 21 and the private key derived from the seed 21 are non-extractable from the secure portion 52.

**[0084]** In a step U3, the signature 121 is further signed with the private certificate key 33 and thus, a certificate signature 133 is generated, which is the signature 121 signed with the private certificate key 33.

**[0085]** In a step U4, the signature 121 may further be signed with the private key 13 and thus, a key signature 133 may be generated, which is the signature 121 signed with the private key 13.

**[0086]** The data processing apparatus 50 may configured (e.g., hard coded) so that private certificate key 33 and private key 13 can only be used to sign data structures that have previously signed by a key derived from the seed 21.

**[0087]** In a step U5, the signature 121, the certificate signature 133 and the key signature 113 (if present) may be output from the data processing apparatus 50, e.g., these data may be broadcast and may be provided, e.g., to a blockchain node to cause a blockchain transaction. However, it should be understood that the present technology is not limited to blockchain implementations, but may also be used in conjunction, e.g., with smart contracts, time stamping, or compliance data.

**[0088]** It will be understood that the seed 21 is generated based on the private certificate key 33 (see Fig. 3). Thus, the signed transaction signature 121 can only be generated when the data processing apparatus 50 has been initialized as described before (as otherwise, the data processing apparatus 50 would not have access to the seed 21). This also applies to the signed transaction signatures 133 and 113, as they are based on the signed transaction signature 121 (based on the seed 21, which in turn is based on a proper initialization). For signed transaction signature 133, the dependency on the proper initialization is further caused by the transaction signature 133 being signed by private certificate key 33, which is also only present on the data processing apparatus 50 after a successful initialization.

**[0089]** As discussed, the data processing apparatus 50 may be configured so that it can only sign digital signatures (e.g., generate signatures 121, 133, and 113), but not sign data structures different to digital signatures. Further still, the data processing apparatus 50 may also be configured so that the private certificate key 33 and the private key 13 can only be used to sign signatures which have been signed by a key derived from seed 21. By limiting the capabilities of which data structure can be signed, the risk of forgery can be greatly reduced.

**[0090]** Furthermore, it will be understood that the data processing apparatus 50 may also output the signed digital certificate 16 and/or the digital system certificate 36 signed with public key 34.

**[0091]** Further embodiments of the present technology are described below with reference to Figures 8 and 10.

**[0092]** It should be understood that Figure 8 an initialization procedure for initializing a data processing apparatus 50. It should further be understood that the initialization steps discussed in conjunction with Figure 8 may be additional steps of the initialization discussed in conjunction with Figure 2a or 2b. That is, the skilled person will understand that the steps described with reference to Fig. 8 can be performed in addition to the steps described with reference to Fig. 2a and/or 2b. However, the initialization steps discussed in conjunction with Fig. 8 may also be performed independently from the steps described in conjunction with Figures 2a and 2b.

**[0093]** Figs. 9 and 10 depict signing procedures which may be performed with the data processing apparatus 50 initialized with the steps depicted in Fig. 8.

**[0094]** More particularly, Fig. 10 depicts a signing procedure generally corresponding to the one discussed with reference to Fig. 4, but including additional features. It will be understood that the signing procedure depicted in Fig. 10 is based on the signing procedure of Fig. 10 with additional steps, as will be discussed below.

**[0095]** Figure 8 again depicts a data processing apparatus 50, which may be the data processing apparatus discussed before, and more particularly steps of its initialization. Furthermore, Fig. 8 also depicts a remote signature system 20. The remote signature system 20 generates a remote asymmetric key pair comprising a remote private key 200 and a remote public key 202. It should be understood that the term "remote" in remote private key 200 and in remote public key 202 should not be limiting as regards the characteristics of these keys, but distinguish these keys 200, 202 from other keys used in the present specification. After the generation of these remote keys 200, 202, the remote public key 202 is sent from the remote signature system 20 to the data processing apparatus 50 and more particularly to the secure portion 52 of the data processing apparatus 50.

**[0096]** Furthermore, signing credentials 220 corresponding to the remote keys 200, 202 are generated and are also send, e.g., to the data processing apparatus 50. For example, the signing credentials may be stored in the secure portion 52 of the data processing apparatus 50. However, it should be understood that this is only exemplary and that the signing credentials 220 may also not be present on the data processing apparatus 50, but may, e.g., be stored elsewhere.

**[0097]** In Fig. 8, it is depicted that the signing credentials 220 and the remote public key 202 are sent to the data processing apparatus 50 individually. However, it should be understood that this is merely exemplary and that the signing credentials 220 and the remote public key 202 can also be sent simultaneously. Furthermore, as it will be understood that the steps described with reference to Fig. 8 also relate to the initialization, it should also be understood that the signing credentials 220 and the remote public key 202 can also be sent simultaneously with the wrapped private certificate key 40 (if the initialization of Fig. 2a and/or 2b is used).

**[0098]** When later providing the signing credentials 220 to the remote signature system 20, the remote signature system 20 will sign a provided data structure, e.g., a transaction request.

**[0099]** It should be understood that the steps depicted in Fig. 8 may be performed in addition to the steps discussed in connection to Figures 2a/2b and 3 (e.g., either before the steps of Figures 2a/2b and 3, simultaneously, or after), however, they may also be performed independently therefrom. If the steps of Fig. 8 are performed in addition to the steps discussed in connection to Figures 2a/2b and 3, the data processing apparatus 50 having undergone the combined initialization process comprises the digital system certificate 36 and the remote public key 202, and (in the secure portion 52) the unwrapped private certificate key 33, the seed 21, and the signing credentials 220.

**[0100]** A further embodiment for generating a signature is depicted in Fig. 9. It will be understood that some steps of the embodiment depicted in Fig. 9 correspond to the steps depicted in Fig. 4 and that corresponding reference signs are used in Figs. 4 and 9.

**[0101]** More particularly, Fig. 9 depicts a signature generation for a data processing apparatus 50 initialized with an initialization procedure comprising the steps discussed in conjunction with Fig. 8.

**[0102]** The data processing apparatus 50 thus has a secure portion 52 and a remote public key 202 is stored in the secure portion 52. Furthermore, signing credentials 220 are used in the signature generation depicted in Fig. 9. The signing credentials 220 may, for example, be stored in the secure portion 52 of the data processing apparatus 50. However, it should be understood that this is optional.

**[0103]** As depicted in Fig. 9, the signature procedure uses a signing request 100. The signing request 100 is provided to the remote signature system 20. Furthermore, the signing credentials 220 are provided to the remote signature system 20. In the depicted embodiment, the signing credentials 220 are provided from the secure portion 52 of the data processing apparatus 50 to the remote signature system 20. However, it should be understood that this is merely exemplary and that the signing credentials 220 may also be provided in a different manner to the remote signature system 20.

**[0104]** The remote signature system 20 comprises a remote private key 200. It should be understood that the term "remote" in remote private key 200 should not be limiting as regards the characteristics of this private key 200, but distinguish this private key 200 from other private keys used in the present specification.

**[0105]** After receiving the correct signing credentials 220, the remote signature system 20 generates a pre-signature 210 based on the signing request 100 and the remote private key 200, to thus generate a pre-signature 210, which is the signing request signed by the remote private key 200. It will thus be understood that the generation of the pre-signature 210 depends on receipt of the correct signing credentials 220.

**[0106]** The signing credentials 220 thus indicate that the remote signature system 20 should provide the pre-signature 210.

**[0107]** In the depicted embodiment, the signing credentials 220 are provided from the data processing apparatus 50 to the remote signature system 20. More particularly, the signing credentials 220 are stored in the secure portion 52 of the data processing apparatus 50. However, it should be understood that this is merely exemplary and that it is also possible that the signing credentials 220 are stored, e.g., on another device and are provided from such other device to the remote signature system 20.

**[0108]** The pre-signature 210 is sent to the data processing apparatus 50 and more particularly to the secure portion 52 of the data processing apparatus 50. Furthermore, also the signing request 100 is provided to the secure portion 52 of the data processing apparatus. For example, the signing request 100 may be sent from the remote signature system

10 to the secure portion 52 of the data processing apparatus 50. However, it should be understood that this is merely exemplary and that the signing request 100 can also be provided to the secure portion 52 of the data processing apparatus 50 in a different manner.

**[0109]** The secure portion 52 of the data processing apparatus 50 comprises the remote public key 202 corresponding to the remote private key 200. By means of the remote public key 202, the data processing apparatus 50 determines whether the pre-signature 210 is valid, i.e., whether the signing request 100 has been signed by the remote private key 200.

**[0110]** If this is the case, at least one signature 250 is generated based on the signing request 100 and a signature routine. For example, at least one signature key and/or seed, together indicated by reference number 260 may be used to generate at least one signature 250 in the secure portion 52. The at least one signature 250 may be broadcast and may be provided, e.g., to a blockchain node 110 to cause a blockchain transaction. However, it should be understood that the present technology is not limited to blockchain implementations, but may also be used in conjunction, e.g., with smart contracts, time stamping, or compliance data.

**[0111]** The embodiments described in conjunction with Figures 8 and 9 thus allow for a different key management. By means of the embodiment described in conjunction with Figures 8 and 9, also the remote signature system 20 is used for signing.

**[0112]** Thus, the remote signature system 20 can be used to lock the signing functionality of the data processing apparatus 50, e.g., in case the data processing apparatus 50 is lost. Put differently, access to the remote signature system 20 may be suppressed, or usage of the remote key pair 200, 210, to thus securely lock the functionality of the data processing apparatus 50. It will be understood that this allows for a temporary or permanent locking of the functionality of the data processing apparatus 50.

**[0113]** For example, in case a data processing apparatus 50 initialized in the above manner was lost, the respective remote key pair 200, 210 can be suppressed at the remote signature system 20. Thus, the data processing apparatus 50 could no longer be used.

**[0114]** Furthermore, a new data processing apparatus 50 could be set up and initialized in the same manner (and in particular with the same seed 21), but with a new remote key pair 200, 210. Thus, a corresponding data processing apparatus 50 could be set up and initialized.

**[0115]** Overall, this embodiment thus allows the data processing apparatus 50 to be remotely activated, deactivated, e.g., temporarily blocked or definitely blocked, and replaced without the need for to replace the seed.

**[0116]** Figure 10 depicts an embodiment of a signature generation generally corresponding to the one depicts in Fig. 9. However, in this embodiment, more details of the signature routine are depicted.

**[0117]** That is, the embodiment in Fig. 10 is one possible realization of the embodiment discussed in Fig. 9, where more details of the signature routine are discussed.

**[0118]** In particular, it will be understood that the process depicted in Fig. 10 is identical to the process depicted in Fig. 9 up to the point where the validity of the pre-signature 210 is determined, and reference can thus be made to the description of Fig. 9 up to this point.

**[0119]** If this is the case, i.e., when it is determined that the signing request 100 has been signed by the remote private key 200, the signing request 100 is subjected to a signature routine comprising the steps described previously with reference to Fig. 4.

**[0120]** In other words, Fig. 10 depicts a combination of the embodiments of Fig. 9 (up to the determination that the signing request 100 has been signed by the remote private key) and Fig. 4 (starting with the provision of the signing request 100 to the secure portion). Thus, the advantages described above with reference to Fig. 4 and Fig. 9 can be combined. Whenever a relative term, such as "about", "substantially" or "approximately" is used in this specification, such a term should also be construed to also include the exact term. That is, e.g., "substantially straight" should be construed to also include "(exactly) straight".

**[0121]** 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.

**[0122]** 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.

Table: Reference numbers used in this specification

| | |
|---|---|
| 11 | Random number generator |
| 12 | Random serial number |
| 13 | Private key |
| 14 | Public key corresponding to private key 13 |
| 15 | Signing request |
| 16 | Signed digital certificate |
| 20 | Remote signature system |
| 21 | Seed for private key generation |
| 33 | Private key generated by certification apparatus, referred to as private certificate key |
| 34 | Public key corresponding to private key 33, referred to as public certificate key |
| 36 | Digital certificate signed with public key 34 |
| 40 | Private key 33 encrypted with public key 14 |
| 50 | Data processing apparatus, e.g., smart card |
| 52 | Secure portion |
| 60 | External data processing apparatus |
| 70 | Data processing system |
| 72 | Further data processing system |
| 80 | User |
| 82 | Personal user data |
| 90 | Certificate signing request |
| 100 | Signing request |
| 110 | Blockchain node |
| 113 | Transaction signature 121 further signed with private key 33 |
| 121 | Transaction signature signed with private key derived from seed 21 |
| 133 | Transaction signature 121 further signed with private key 13 |
| 200 | Remote private key |
| 202 | Remote public key |
| 210 | Pre-signature |
| 220 | Signing credentials |
| 250 | At least one signature |
| 260 | Signature key and/or seed |

## Claims

**1.** A data processing apparatus (50) comprising a secure portion (52),

wherein the secure portion (52) comprises

a private key (13),
an unencrypted private certificate key (33), and
a seed (21) generated based on a private certificate key (33),

wherein the private key (13), the unencrypted private certificate key (33), and the seed (21) are non-extractable from the secure portion (52).

**2.** The data processing apparatus (50) according to claim 1, wherein the data processing apparatus (50) comprises a signed digital certificate (16).

**3.** The data processing apparatus (50) according to any of the preceding claims, wherein the secure portion (52) comprises a random number generator (11)

**4.** The data processing apparatus (50) according to claim 3, wherein the data processing apparatus comprises a serial number (12) generated by the random number generator (11).

**5.** The data processing apparatus (50) according to any of the preceding claims, wherein the data processing apparatus (50) is a smart card, wherein the smart card preferably has near field communication functionality.

**6.** The data processing apparatus (50) according to any of the preceding claims, wherein the data processing apparatus (50) comprises a signed digital system certificate (36), wherein the signed digital system certificate (36) is signed with a public certificate key (34) corresponding to the private certificate key (33), and wherein the signed digital system certificate (36) is based on personal user data (82), the signed digital certificate (16) and the public certificate key (34).

**7.** The data processing apparatus (50) according to any of the preceding apparatus claims, wherein the data processing apparatus (50) is obtainable by a method, wherein the method comprises

providing a data processing apparatus (50), wherein the data processing apparatus (50) comprises the secure portion (52), wherein the secure portion (52) comprises the private key (13) that cannot be extracted from the secure portion (52), wherein the secure portion (52) comprises a public key (14) corresponding to the private key (13),
the data processing apparatus providing a signing request (15), the public key (14), and a serial number (12),
based on the signing request (15), the public key (14), and the signing request (15), an external data processing apparatus (60) generating a signed digital certificate (16), and
providing the signed digital certificate (16) to the data processing apparatus (50), providing the signed digital certificate (16) to a data processing system (70),
the data processing system (70) receiving personal user data (82) from a user (80), providing a public certificate key (34) to the data processing system (70),
the data processing system (70) generating a signed digital system certificate (36) signed with the public certificate key (34) based on the personal user data (82), the signed digital certificate (16), and the public certificate key (34),
providing the signed digital system certificate (36) to the data processing apparatus (50),
generating the public certificate key (34) and the corresponding private certificate key (33),
encrypting the private certificate key (33) with the public key (14) and thus generating a wrapped key (40), and providing the wrapped key (40) to the secure portion (52) of the data processing apparatus,
in the secure portion (52), unencrypting the wrapped key (40) with the private key (13) and thus obtaining the private certificate key (33),
in the secure portion (52), generating the seed (21) based on the private certificate key (33).

**8.** The data processing apparatus (50) according to any of the preceding claims, wherein the data processing apparatus (50) is configured to only allow data structures signed by a key derived from seed (21) to be signed by the unencrypted private certificate key (33).

**9.** The data processing apparatus (50) according to any of the preceding claims, wherein the data processing apparatus (50) is configured to only allow data structures signed by a key derived from seed (21) to be signed by the private key (13).

**10.** The data processing apparatus (50) according to any of the preceding claims, wherein the secure portion (52) comprises a remote public key (202).

**11.** A method, wherein the method uses the data processing apparatus (50) according to any of the preceding claims, the method comprising

the secure portion (52) receiving a signing request (100),
in the secure portion (52), generating a signature (121) signed with a private key derived from the seed (21) and signing the signature (121) with the unencrypted private certificate key (33) and thus generating a signature (133) signed with the unencrypted private certificate key (33),
outputting the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key (33).

**12.** The method according to claim 11, wherein the method further comprises

in the secure portion (52), signing the signature (121) with the private key (13) and thus generating a signature (113) signed with the private key (13),
outputting the signature (113) signed with the private key (13) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

**13.** The method according to any of the 2 preceding claims, wherein the method uses the data processing apparatus (50) according to any of the claims 1 to 10 with the features of claim 2,
wherein the method further comprises outputting the signed digital certificate (16) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

**14.** The method according to any of the 3 preceding claims, wherein the method uses the data processing apparatus (50) according to any of the claims 1 to 10 with the features of claim 7,
wherein the method further comprises outputting the signed digital system certificate (36) together with the signature (121) signed with the private key derived from the seed (21) and the signature (133) signed with the unencrypted private certificate key.

**15.** The method according to any of the 4 preceding embodiments, wherein the method uses the data processing apparatus (50) according to claim 10, wherein the method further comprises

a remote signature system (20) receiving the signing request (100),
the remote signature system (20) signing the signing request (100) with a remote private key (200) corresponding to the remote public key (202) and thus generating a pre-signature (210),
the secure portion (52) receiving the pre-signature (210), and
in the secure portion (52) verifying with the remote public key (202) that the pre-signature (210) is the signing request (100) signed with the remote private key (200),
wherein generating the at least one signature (121, 133, 113, 250) in the secure portion (52) and outputting the at least one signature (121, 133, 113, 250) depend on the successful verification that the pre-signature (210) is the signing request (100) signed with the remote private key (200) with the remote public key (202).

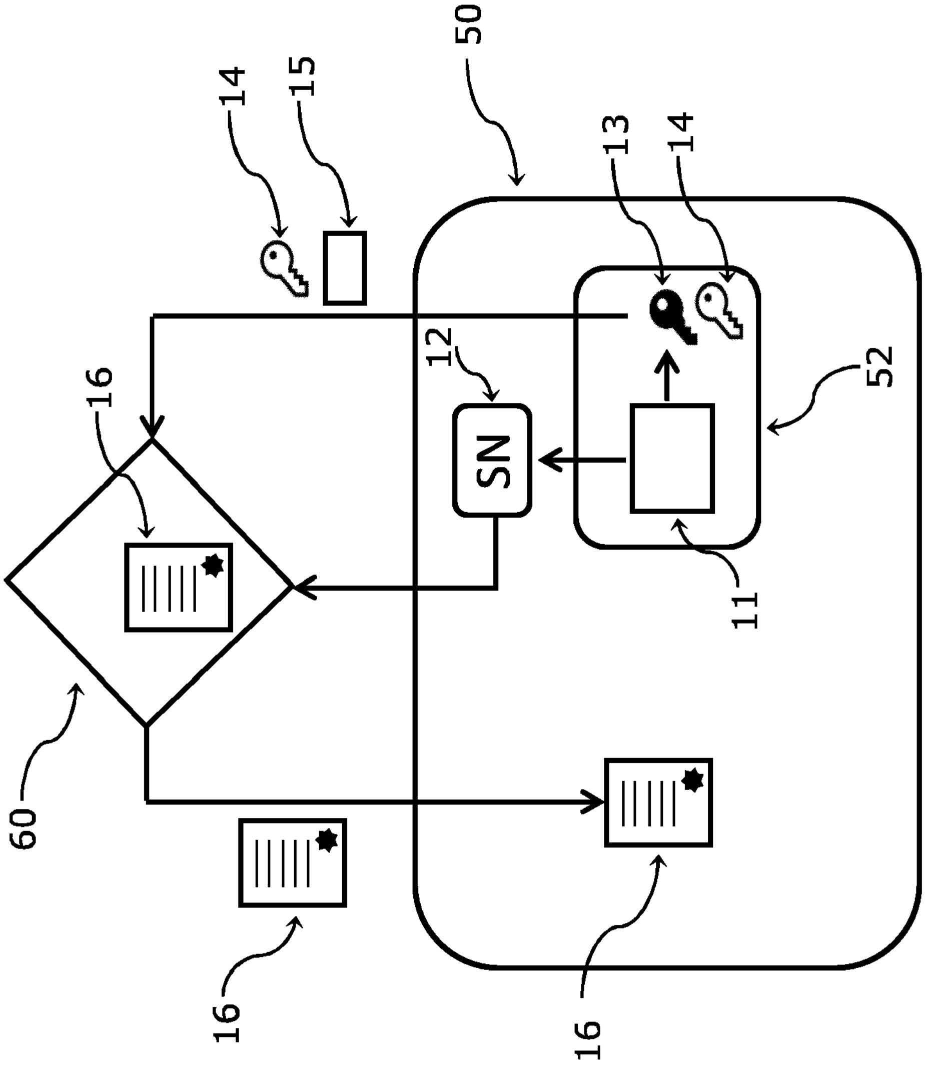

Fig. 1

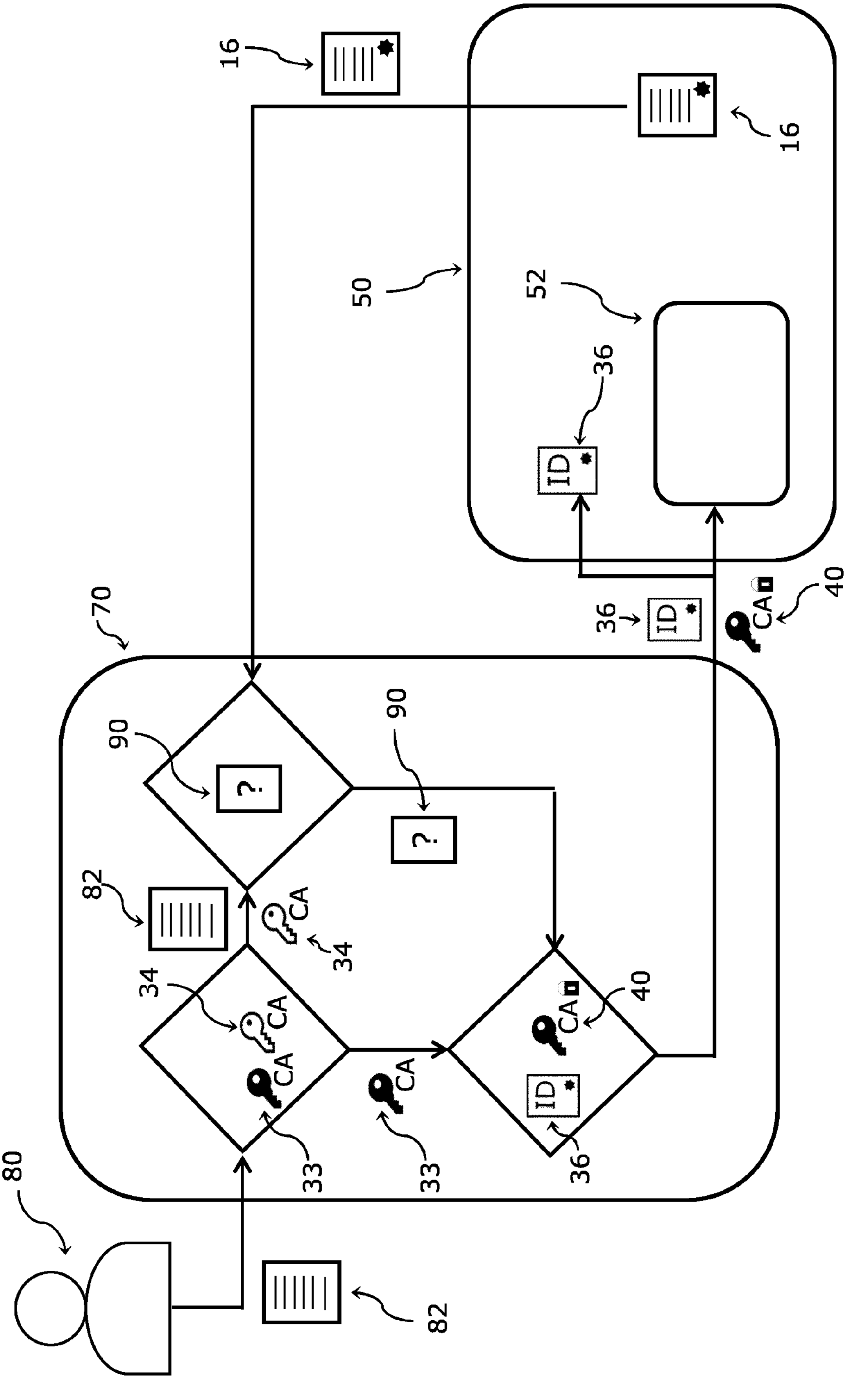
16
16
50
52
36
ID
36
ID
40
CA
70
90
?
90
?
82
34
CA
34
CA
CA
40
CA
ID
33
33
36
80
82

Fig. 2a

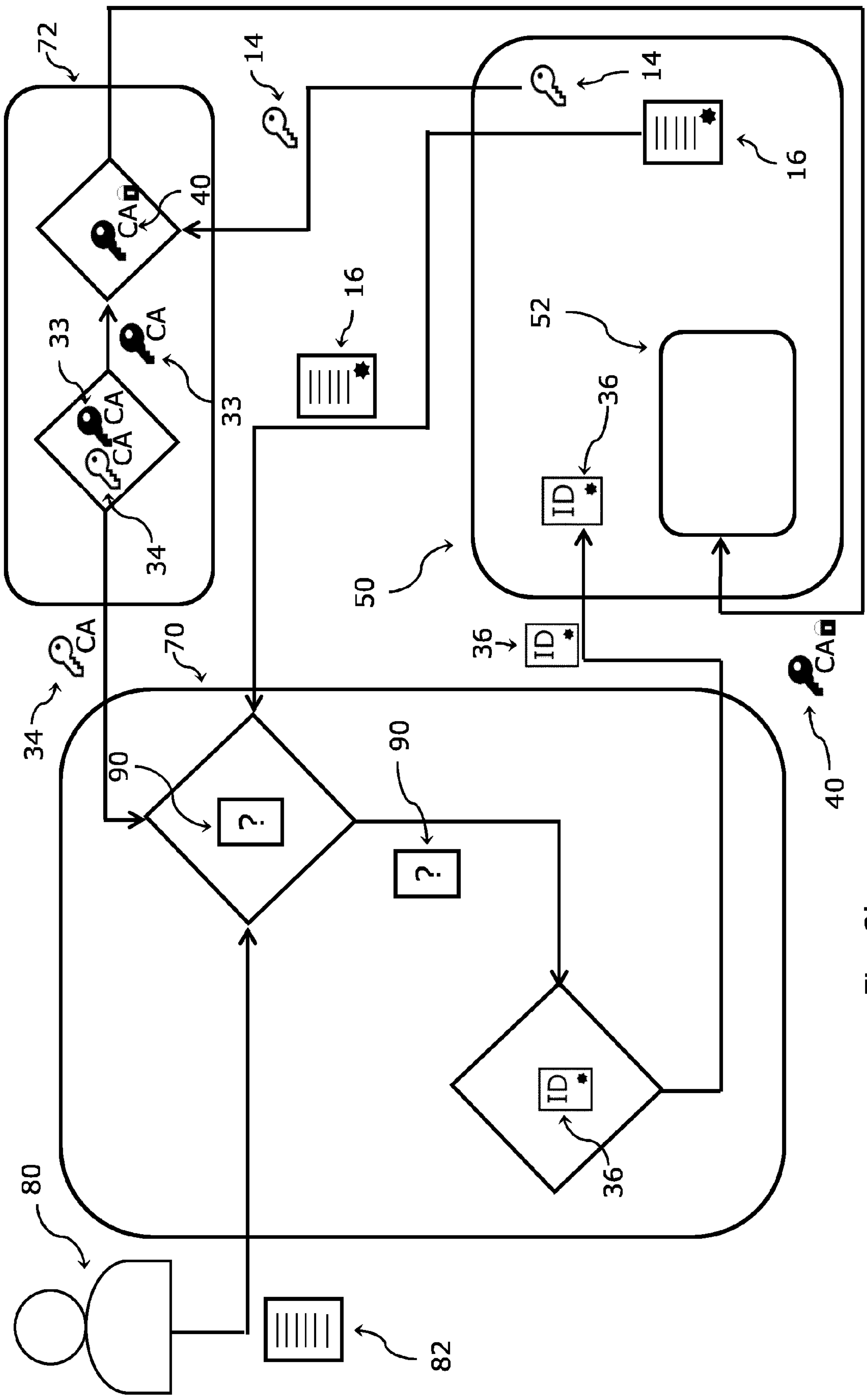
72
14
CA
40
33
CA
33
CA
CA
34
16
14
16
52
36
ID
50
36
ID
CA
40
34
CA
70
90
?
90
?
ID
36
80
82

Fig. 2b

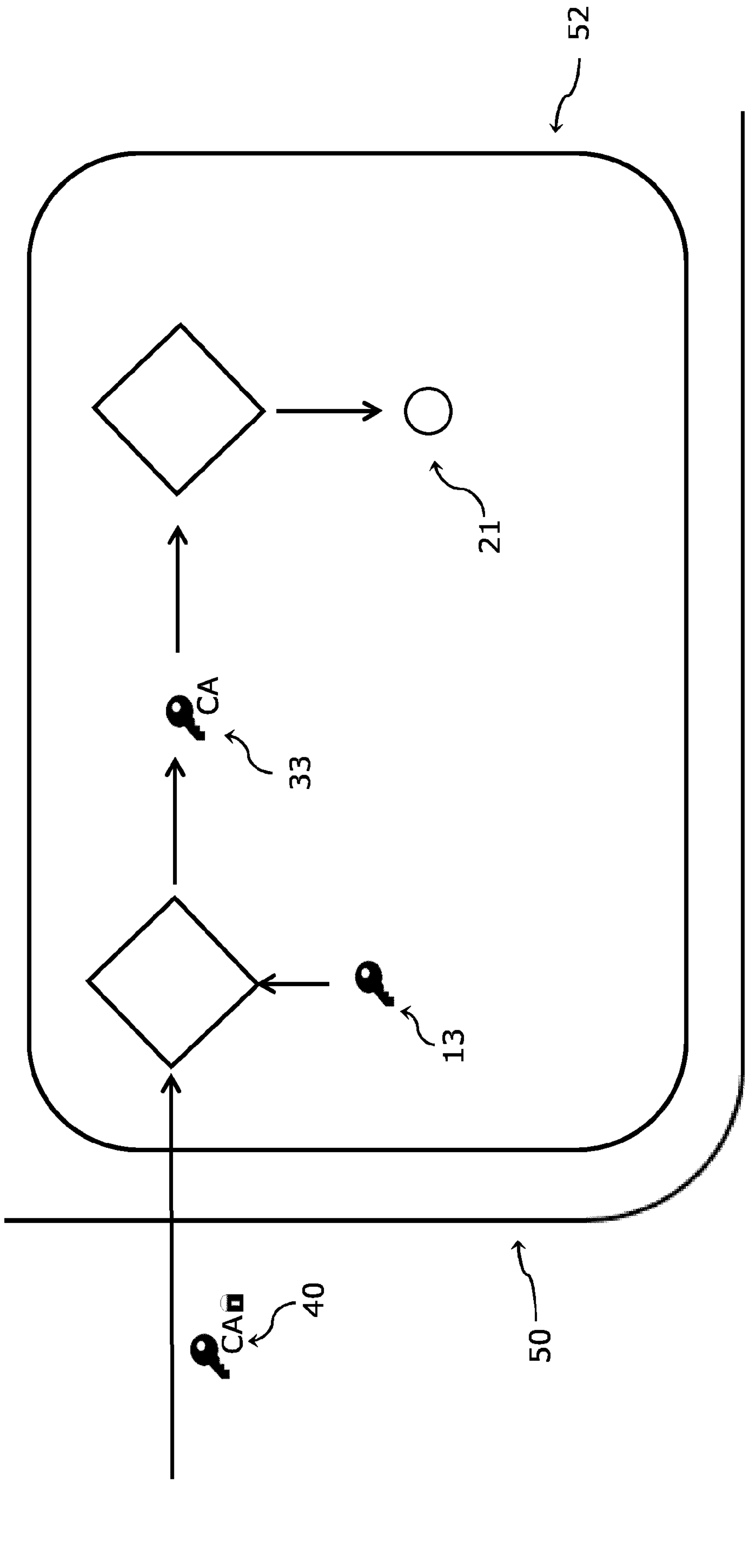

Fig. 3

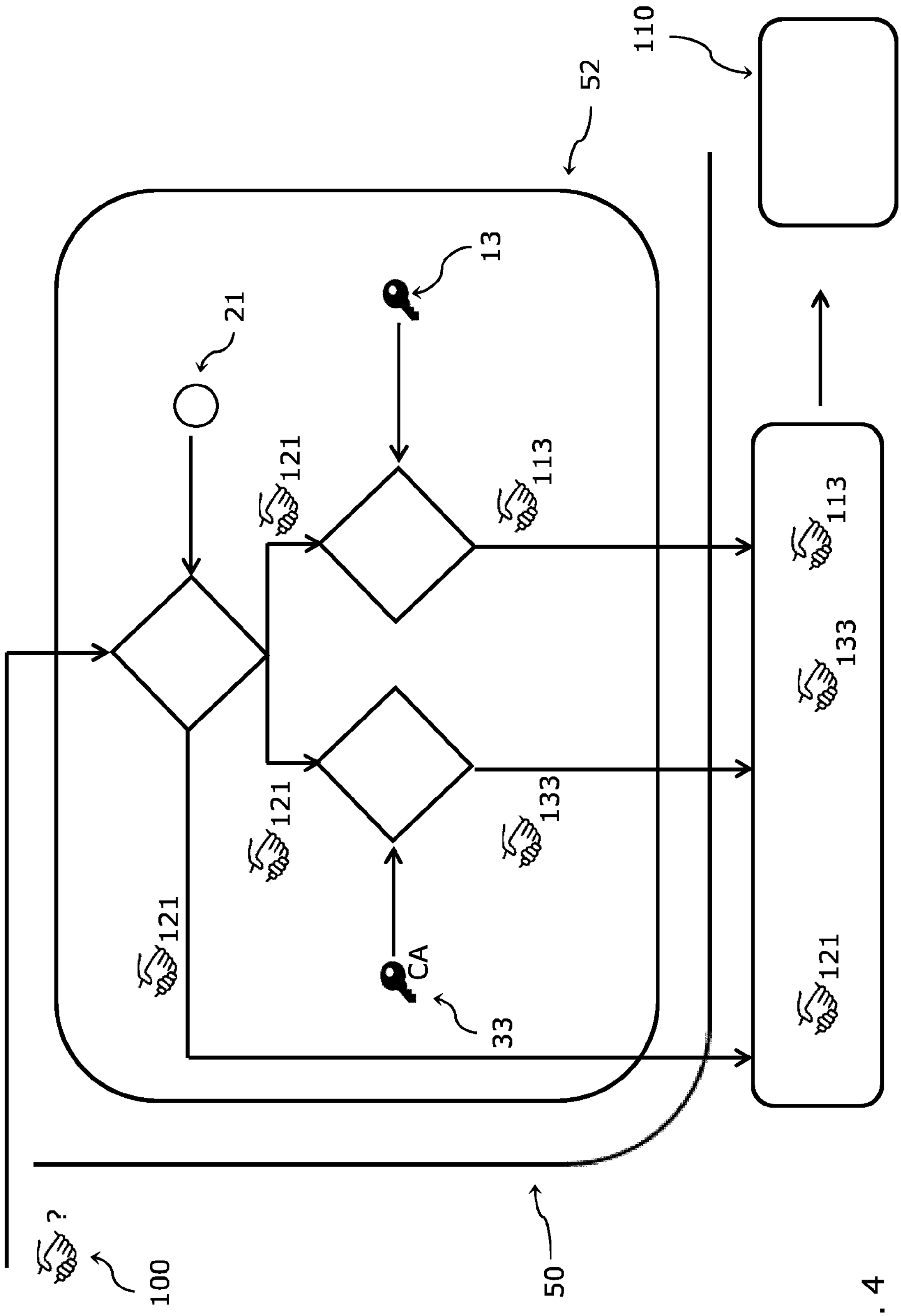

Fig. 4

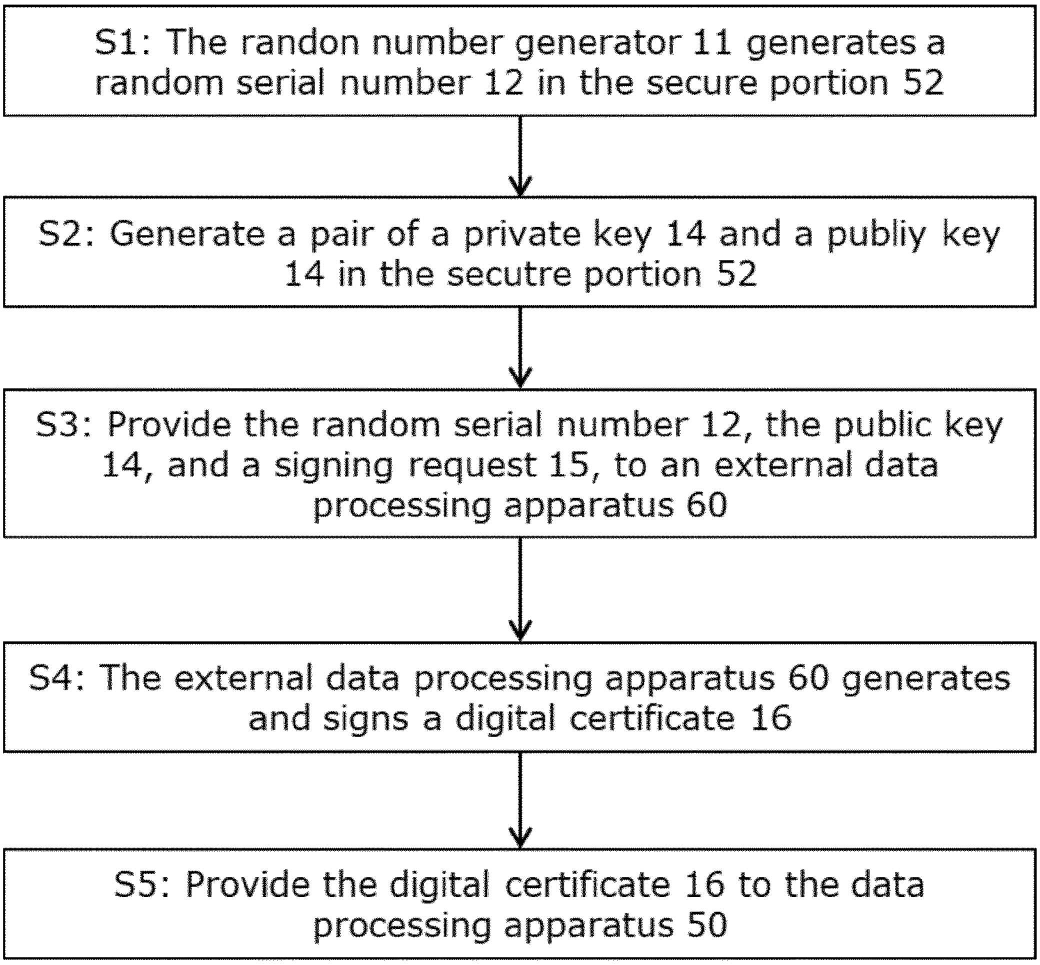
S1: The randon number generator 11 generates a random serial number 12 in the secure portion 52
S2: Generate a pair of a private key 14 and a publiy key 14 in the secutre portion 52
S3: Provide the random serial number 12, the public key 14, and a signing request 15, to an external data processing apparatus 60
S4: The external data processing apparatus 60 generates and signs a digital certificate 16
S5: Provide the digital certificate 16 to the data processing apparatus 50

Fig. 5

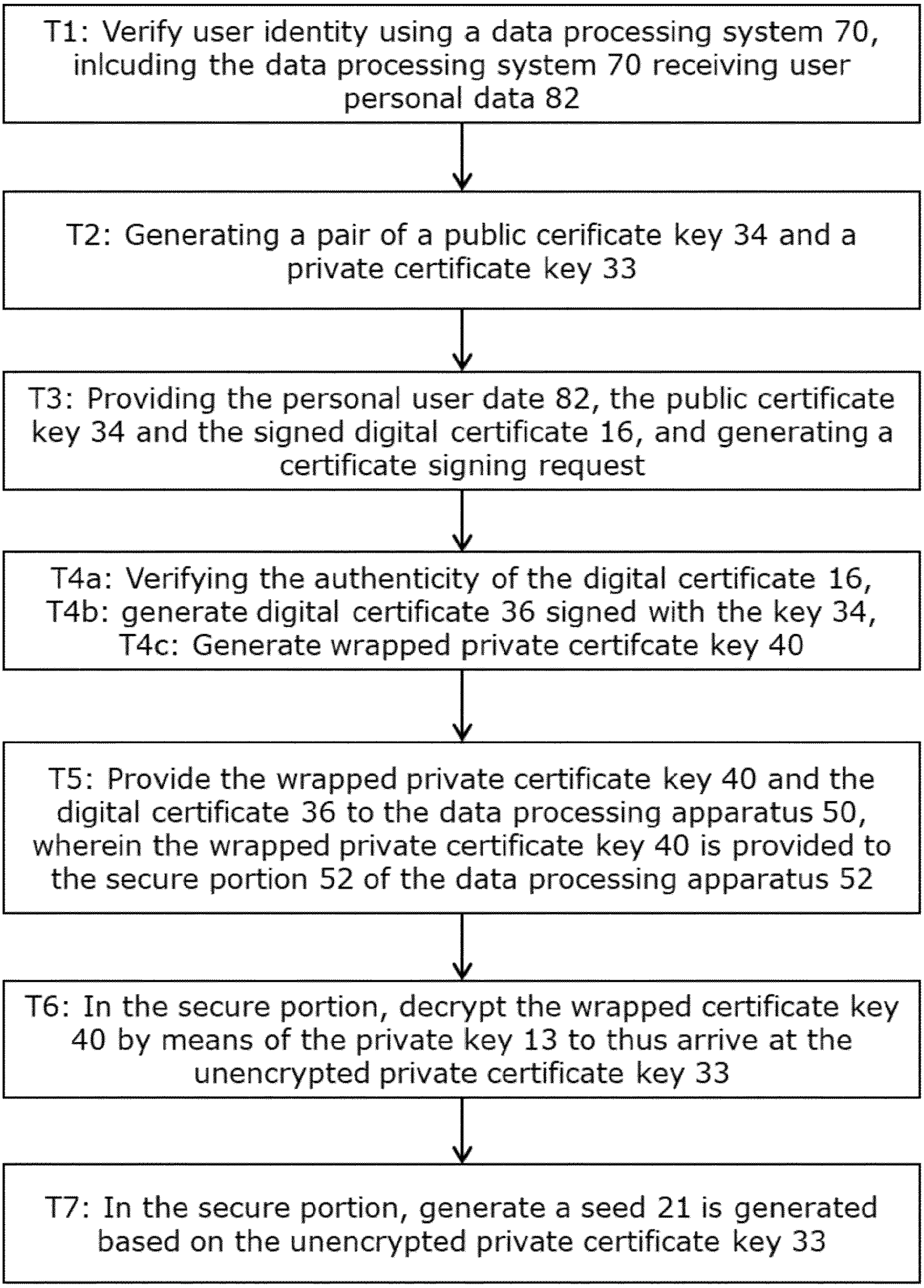
T1: Verify user identity using a data processing system 70, inlcuding the data processing system 70 receiving user personal data 82
T2: Generating a pair of a public cerificate key 34 and a private certificate key 33
T3: Providing the personal user date 82, the public certificate key 34 and the signed digital certificate 16, and generating a certificate signing request
T4a: Verifying the authenticity of the digital certificate 16, T4b: generate digital certificate 36 signed with the key 34, T4c: Generate wrapped private certifcate key 40
T5: Provide the wrapped private certificate key 40 and the digital certificate 36 to the data processing apparatus 50, wherein the wrapped private certificate key 40 is provided to the secure portion 52 of the data processing apparatus 52
T6: In the secure portion, decrypt the wrapped certificate key 40 by means of the private key 13 to thus arrive at the unencrypted private certificate key 33
T7: In the secure portion, generate a seed 21 is generated based on the unencrypted private certificate key 33

Fig. 6

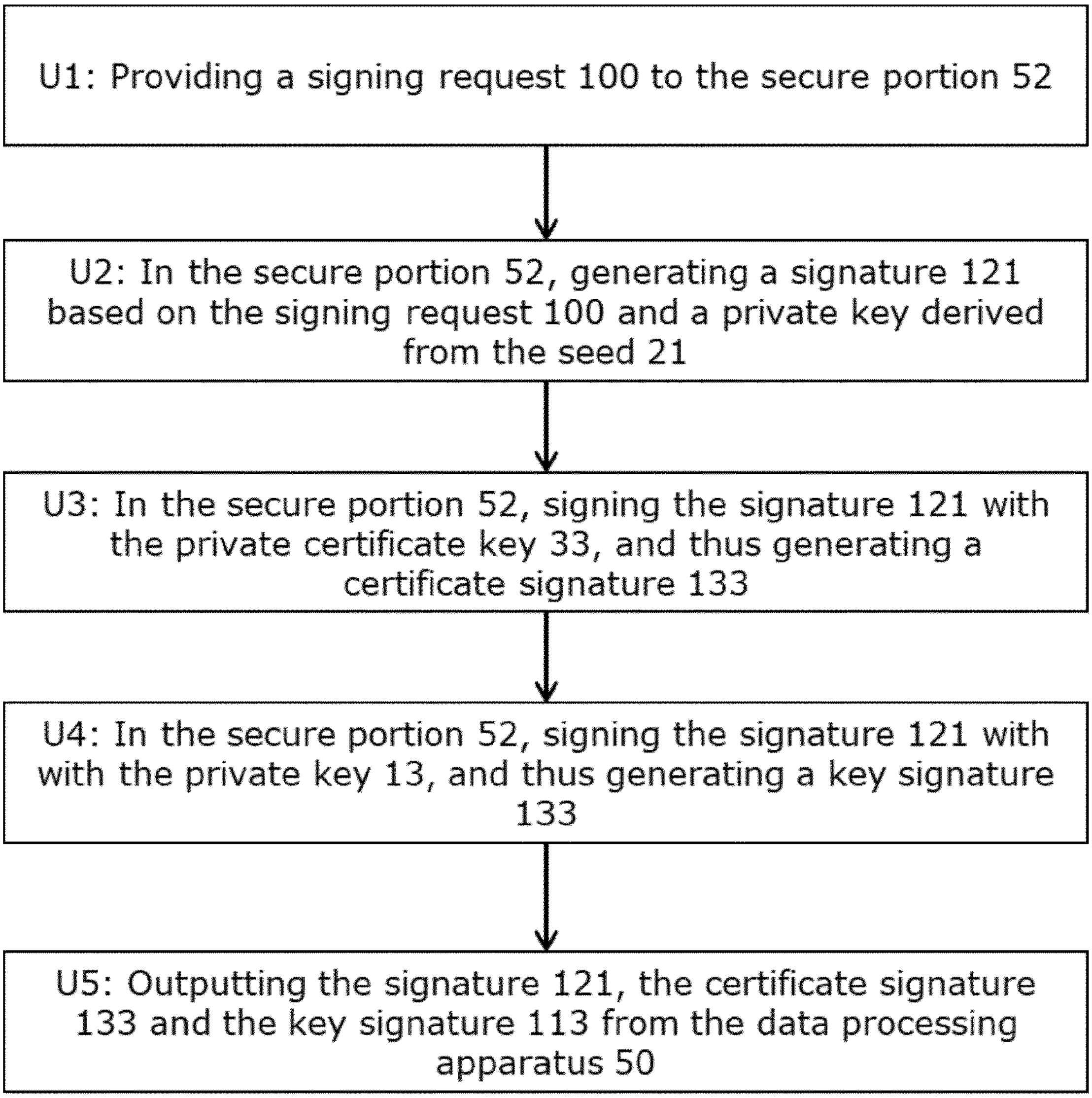
U1: Providing a signing request 100 to the secure portion 52
U2: In the secure portion 52, generating a signature 121 based on the signing request 100 and a private key derived from the seed 21
U3: In the secure portion 52, signing the signature 121 with the private certificate key 33, and thus generating a certificate signature 133
U4: In the secure portion 52, signing the signature 121 with with the private key 13, and thus generating a key signature 133
U5: Outputting the signature 121, the certificate signature 133 and the key signature 113 from the data processing apparatus 50

Fig. 7

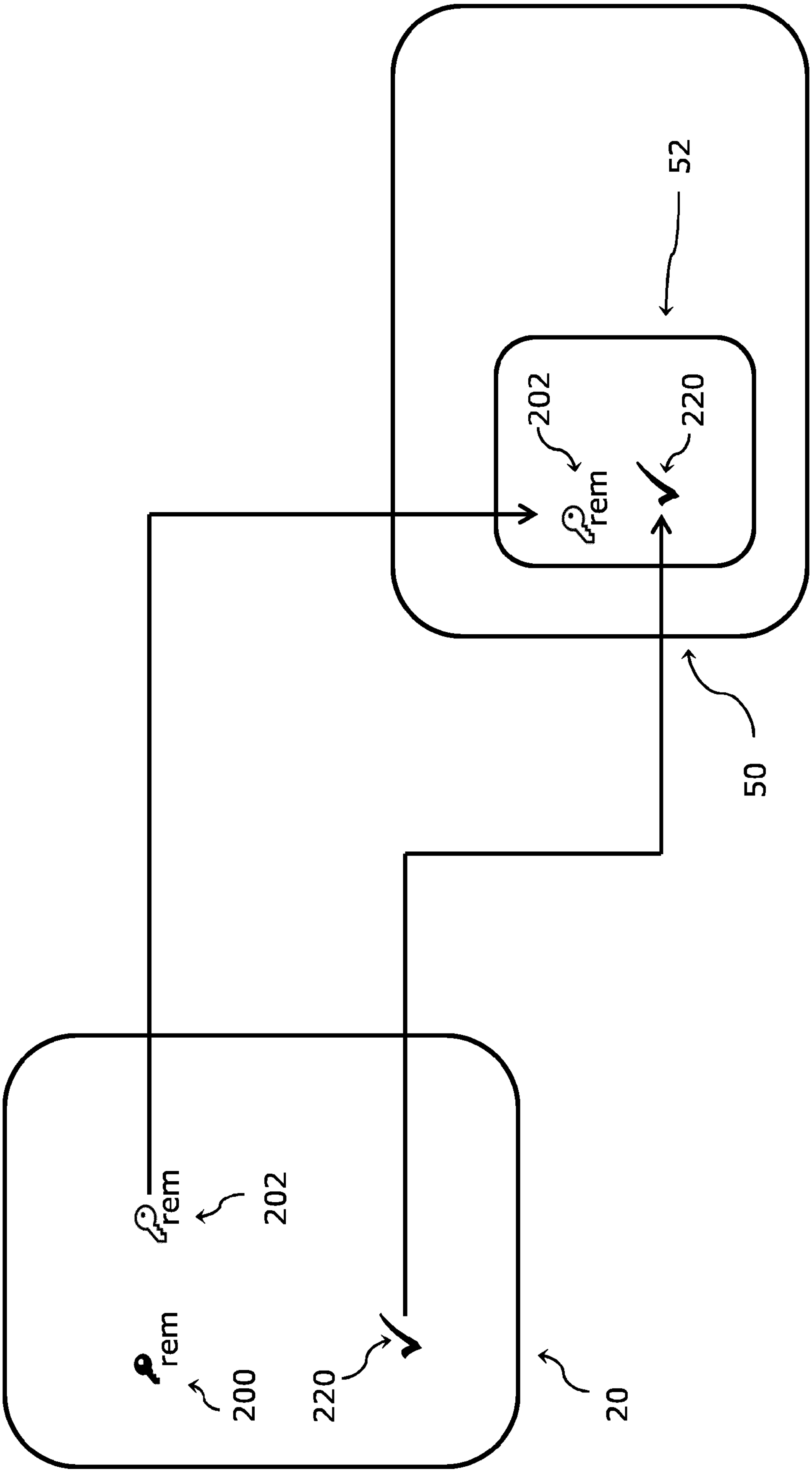

Fig. 8

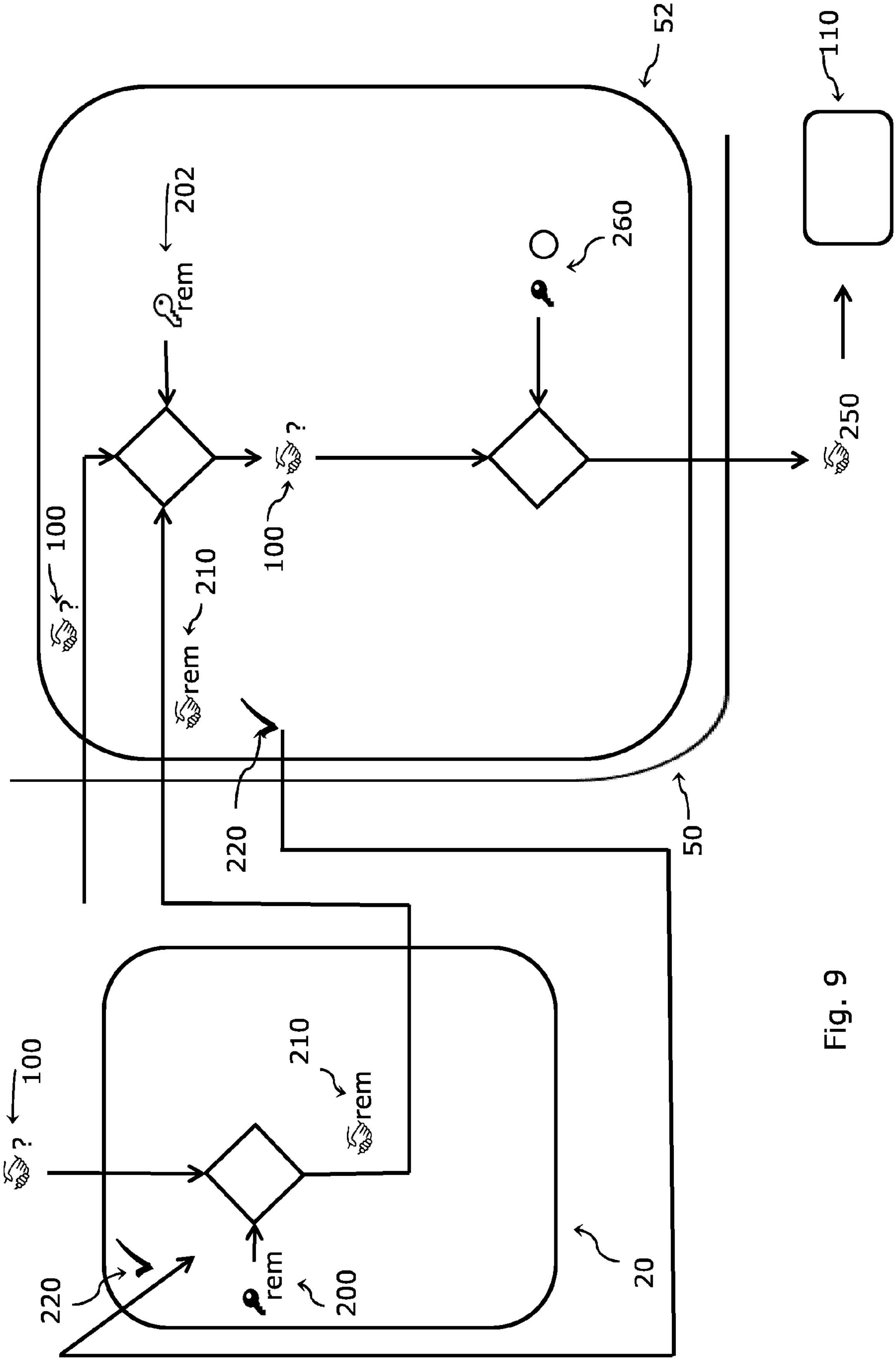
52
110
202
rem
260
100
?
210
rem
100
?
250
220
50
100
?
210
rem
220
rem
200
20

Fig. 9

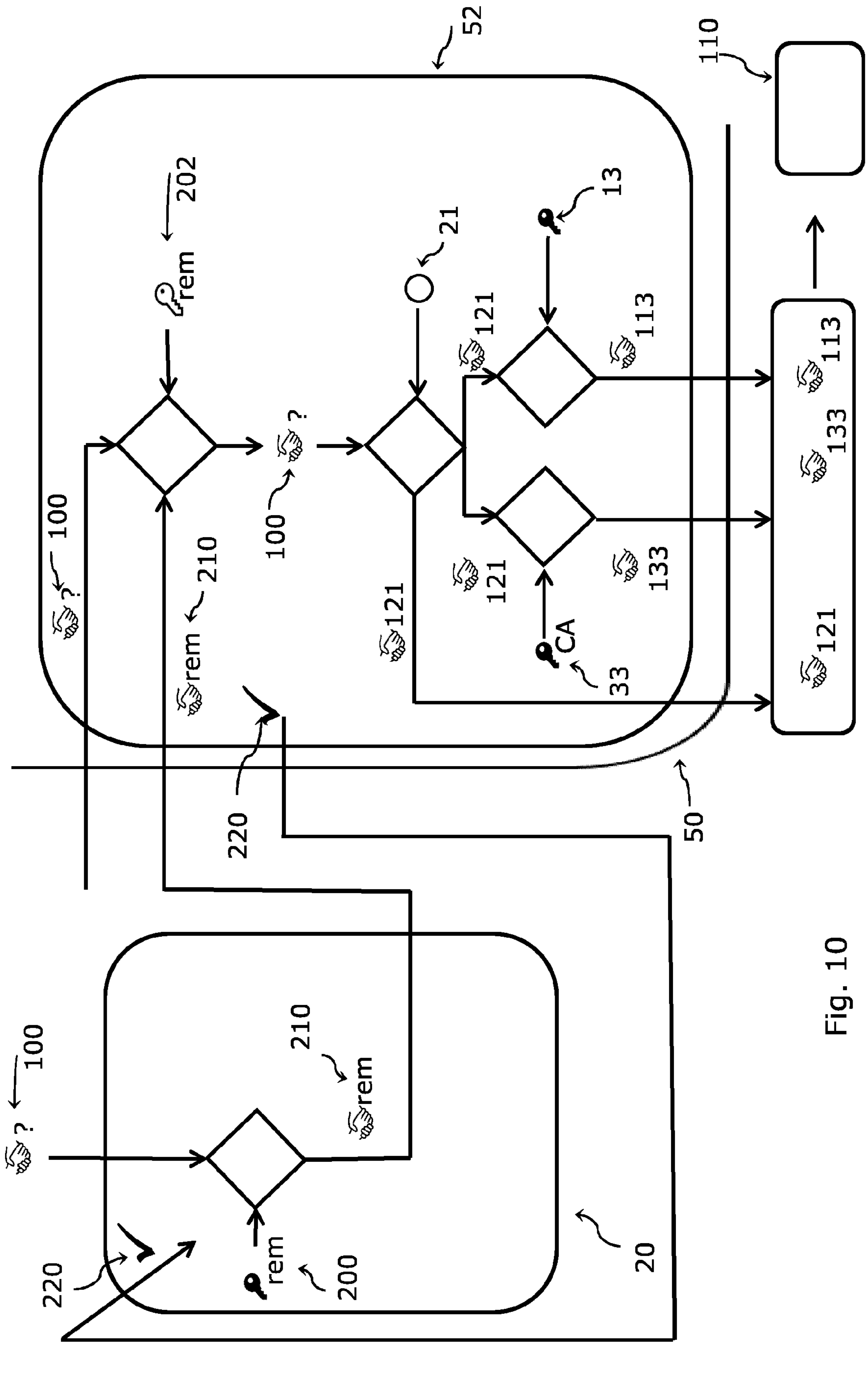
52
202
rem
21
13
110
121
113
100
?
121
133
113
133
121
210
rem
121
CA
33
220
50
100
?
210
rem
220
rem
200
20

Fig. 10

Europäisches Patentamt
European Patent Office
Office européen des brevets

# EUROPEAN SEARCH REPORT

Application Number
EP 22 15 0341

## 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 | US 2018/262341 A1 (CHENG GANG [US] ET AL) 13 September 2018 (2018-09-13) | 1-10 | INV.<br>G06F21/71<br>G06F21/64<br>H04L9/32<br>H04L9/40 |
| Y | * abstract; figures 1, 4, 5, 6, 7, 8 *<br>* claim 1 *<br>* paragraphs [0024], [0026] *<br>* paragraphs [0032] - [0035] *<br>* paragraphs [0057] - [0065] *<br>----- | 11-15 | |
| Y | WO 2014/106181 A2 (VASCO DATA SECURITY INC [US]; VASCO DATA SECURITY INT GMBH [CH]) 3 July 2014 (2014-07-03) | 11-15 | |
| A | * abstract; figures 1, 2 *<br>* paragraphs [0027], [0028], [0034] *<br>* paragraphs [0078], [0082], [0083] *<br>* paragraphs [0086], [0096] *<br>----- | 1-10 | |
| X | EP 3 474 209 A1 (KONINKLIJKE KPN NV [NL]) 24 April 2019 (2019-04-24) | 1-10 | |
| A | * abstract; figures 1a, 1b, 1c, 1d, 3, 5 *<br>* paragraphs [0007] - [0010] *<br>* paragraphs [0033] - [0040] *<br>* paragraphs [0056] - [0058] *<br>* paragraphs [0060], [0062], [0079] *<br>----- | 11-15 | |

TECHNICAL FIELDS SEARCHED (IPC)

H04L
H04W
G06F

The present search report has been drawn up for all claims

1

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| Munich | 17 June 2022 | Schossmaier, Klaus |

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

# ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 22 15 0341

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.

17-06-2022

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2018262341 A1 | 13-09-2018 | NONE | |
| WO 2014106181 A2 | 03-07-2014 | US 2014195811 A1<br>WO 2014106181 A2 | 10-07-2014<br>03-07-2014 |
| EP 3474209 A1 | 24-04-2019 | EP 3474209 A1<br>US 2019121988 A1 | 24-04-2019<br>25-04-2019 |

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