



(51) International Patent Classification:

H04L 9/40 (2022.01)

H04L 9/00 (2022.01)

H04L 9/32 (2006.01)

G06F 21/31 (2013.01)

(21) International Application Number:

PCT/EP2023/062045

(22) International Filing Date:

05 May 2023 (05.05.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

22172694.6

11 May 2022 (11.05.2022)

EP

(71) Applicant: SONY GROUP CORPORATION [JP/JP];

1-7-1 Konan Minato-ku, Tokyo, 108-0075 (JP).

(71) Applicant (for AL only): SONY EUROPE B.V. [GB/GB];

The Heights, Brooklands, Weybridge (Surrey) KT13 0XW (GB).

(72) Inventor: CLAESEN, Rik; c/o Sony Europe B.V.,

Zweigniederlassung Deutschland, Stuttgart Technology Center, Hedelfinger Str. 61, 70327 Stuttgart (DE).

(74) Agent: 2SPL PATENTANWÄLTE PARTG MBB; Lan-

daubogen 3, 81373 München (DE).

(81) Designated States (unless otherwise indicated, for every

kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: AUTHENTICATION DEVICE, METHOD, AND COMPUTER PROGRAM

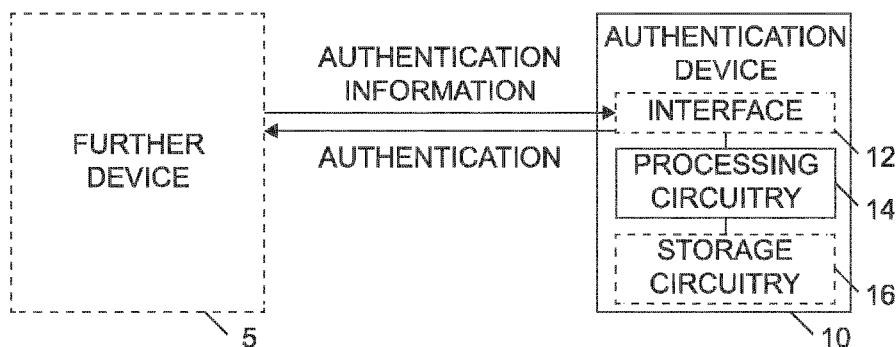


Fig. 1a

(57) Abstract: Various examples of the present disclosure relate to an authentication device, method, and computer program, to a device, such as a web server or a machine, comprising the authentication device, and to a web service executing the authentication method. The authentication device comprises an interface for communicating with a further device. The authentication device comprises processing circuitry configured to obtain authentication information from the further device. The authentication information comprises information for identifying a non-fungible token linked to an authentication identity of an owner of the further device. The processing circuitry is configured to authenticate the further device vis-à-vis the authentication device based on the information for identifying the non-fungible token.



Authentication Device, Method, and Computer Program

Field

5

Various examples of the present disclosure relate to an authentication device, method, and computer program, to a device, such as a web server or a machine, comprising the authentication device, and to a web service executing the authentication method.

10

Background

15

Today, users are confronted with login identifiers (such as usernames, email addresses, phone numbers etc.) and passwords for authentication when accessing websites or other internet-based services. Due to the multitude of services that users use, they tend to re-use passwords, use easy to remember passwords, or even write them down, which is not a good security practice. A minority uses a password manager, but even that requires remembering a master password. Moreover, the storage and protection of these passwords pose a challenge for the services that require them. For hackers and other criminals, the concentration of passwords is known as “honey pot” for which the effort is worth the price.

20

There may be a desire for an improved concept for authenticating a user.

Summary

25

This desire is addressed by the subject-matter of the independent claims.

30

Various examples of the present disclosure are based on the finding that NFTs (Non-Fungible Tokens) have properties that make them suitable for use in authentication. In particular, NFTs are linked to their owner’s address on the blockchain (a particular implementation of a distributed ledger, as used by Ethereum and Bitcoin), so that the link between the NFT and the owner can be easily verified. Moreover, the address at which the NFT is accessible on the blockchain is derived from a public key of the owner. Through the mechanics of key pair-based cryptography, the owner can, using the corresponding private key, generate and provide information that authenticates the owner as the owner of the NFT. This mechanism can be

used to register and authenticate a user on multiple websites or internet services using a single NFT that the user owns, without needing to use any password in the process, which may address the above-mentioned password-related shortcomings. As no password is needed for authentication, the same NFT can be re-used for authentication with other services. The proposed approach may also eliminate the challenges linked to safely storing passwords for the different web services, as there might be no more passwords to store.

Some aspects of the present disclosure relate to an authentication device. The authentication device comprises an interface for communicating with a further device. The authentication device comprises processing circuitry configured to obtain authentication information from the further device. The authentication information comprises information for identifying a non-fungible token linked to an authentication identity of an owner of the further device. The processing circuitry is configured to authenticate the further device vis-à-vis the authentication device based on the information for identifying the non-fungible token. In other words, the NFT of the user is used to authenticate the user vis-à-vis the authentication device, which may eliminate the use of passwords and thus the aforementioned shortcomings.

In some examples, the authentication information further may comprise a cryptographic signature. The processing circuitry may be configured to verify the cryptographic signature based on the information for identifying the non-fungible token. The authentication may be successful if the verification of the cryptographic signature is successful. The cryptographic signature may be used to prove that the owner of the further device is the owner of the non-fungible token.

To avoid damage if an attacker should manage to intercept the authentication information, the authentication may be performed based on a challenge that is provided by the authentication device to the further device. For example, the processing circuitry may be configured to provide challenge information to the further device, with the cryptographic signature being generated based on the challenge information. For example, the challenge information may comprise a unique one-time code. This challenge information may change for each authentication, such that the interception of one unit of authentication information is worthless for subsequent authentication attempts.

In general, the proposed concept may be used between an authentication device that is part of a server and a client device, which may communicate via a computer network, such as the internet. Accordingly, the processing circuitry may be configured to provide the challenge information to the further device via a computer network.

5

Alternatively (or additionally), the processing circuitry may be configured to provide the challenge information to the further device as a two-dimensional visual code being displayed on a display device. This may enable authentication in scenarios where the further device attempts to authenticate with an authentication device in situ, i.e., in physical proximity with the device comprising the authentication device.

10

In some examples, the processing circuitry may be configured to use the information for identifying the non-fungible token to obtain a cryptographic key linked to the authentication identity of the owner of the further device, and to authenticate the further device based on the cryptographic key. For example, the processing circuitry may be configured to obtain the cryptographic key from a storage device of the authentication device. The cryptographic key linked to the authentication identity of the owner may be used to verify a component of the authentication information, e.g., a response to the challenge information mentioned above, in order to prove that the authentication is performed by the owner of the non-fungible token.

20

In some examples, the processing circuitry may be configured to obtain the cryptographic key from a device of the owner of the further device (such as the further device or another device) during registration of the authentication identity at the authentication device, and to store the cryptographic key using the storage device. In other words, storing the cryptographic key may be part of the registration process, laying the groundwork for subsequent verification of a response to the challenge information provided during authentication.

25

Non-fungible tokens can be used to authenticate their owner as they are (publicly) linked with their owner, with the link being verifiable via publicly available information. For example, the processing circuitry may be configured to verify the link between the non-fungible token and the authentication identity using the cryptographic key. This may avoid account takeovers in scenarios where a non-fungible token previously used for authentication is transferred to a different user.

30

In some examples, the processing circuitry may be configured to verify the link between the non-fungible token and the authentication identity based on an address of the non-fungible token on a distributed ledger, with the authentication being successful if the address of the non-fungible token is derivable from the cryptographic key. Additionally, or alternatively, the processing circuitry may be configured to verify a cryptographic signature that is part of the authentication information using the cryptographic key, with the authentication being successful if the verification of the cryptographic signature may be successful. In other words, the cryptographic key, which may be a public key of a key pair associated with the cryptocurrency wallet of the owner, may hold two components of the proposed authentication scheme together – it can be used to verify that the authentication information is provided by the holder of a corresponding private key (as the response to the challenge information can be verified using the cryptographic key), and it can be used to verify the link between the non-fungible token and the owner (as the non-fungible token's address can be derived from the cryptographic key).

15

As mentioned above, the cryptographic key may be a public key of a key pair of the owner of the further device, with the authentication being successful if the cryptographic signature is generated using a private key of the key pair (and if the address of the non-fungible token on the distributed ledger is derivable from the cryptographic key). Accordingly, the address of the non-fungible token on the distributed ledger may be derivable from the cryptographic key. Thus, the public key may be used to verify that the authentication is being performed by the owner of the non-fungible token.

20

In general, the information for identifying the non-fungible token may be any kind of information that is suitable for identifying the non-fungible token. In various examples, the information for identifying a non-fungible token may be an address of the non-fungible token on the distributed ledger. Alternatively (or additionally), the information for identifying a non-fungible token may be an identifier of the non-fungible token. While the address of the non-fungible token on the distributed ledger provides a more direct link to the cryptocurrency wallet of the owner, it can also be derived from a directory linking identifiers of non-fungible tokens to their corresponding addresses on the distributed ledger.

25

30

Another aspect of the present disclosure relates to a corresponding authentication method. The authentication method comprises obtaining authentication information from a device.

The authentication information comprises information for identifying a non-fungible token linked to an authentication identity of an owner of the device. The authentication method comprises authenticating the device based on the information for identifying the non-fungible token.

5

Another aspect of the present disclosure relates to a corresponding authentication computer program having a program code for performing the above authentication method, when the computer program is executed on a computer, a processor, or a programmable hardware component.

10

The proposed concept may be used in different scenarios. For example, an aspect of the present disclosure relates to a web server comprising the above authentication device. Similarly, another aspect of the present disclosure relates to a web service performing the above authentication method. Since the distributed ledger and the non-fungible token are generally accessible via the internet, providing a direct link that can be used for verification, a seamless authentication experience can be provided for authenticating vis-à-vis a web server or web service.

15

Another scenario relates to tangible devices, such as machines. Accordingly, an aspect of the present disclosure relates to a machine comprising the above authentication device. For example, the machine may be a transportation device (such as a rental car, a rental scooter, a rental bike, or a public transportation vehicle, turnstile, or check-in point) or a self-service vending device. Such devices also benefit from a non-fungible token-based authentication approach, as funds or a membership can be linked to the NFT and accessed by proving ownership of the NFT.

20

25

Brief description of the Figures

30

Some examples of apparatuses and/or methods will be described in the following by way of example only, and with reference to the accompanying figures, in which:

Fig. 1a shows a block diagram of an example of an authentication device;

Fig. 1b shows a flow chart of an example of an authentication method;

Fig. 1c shows a flow chart of an example of a method for initial registration prior to authentication;

5 Fig. 2 shows a block diagram of an example of a web server comprising an authentication device;

Fig. 3 shows a schematic diagram of an example of a rental scooter comprising an authentication device; and

10

Fig. 4 shows a diagram of an example of actions used to register or authenticate a user on a website or internet-based service using an NFT.

Detailed Description

15

Some examples are now described in more detail with reference to the enclosed figures. However, other possible examples are not limited to the features of these embodiments described in detail. Other examples may include modifications of the features as well as equivalents and alternatives to the features. Furthermore, the terminology used herein to describe certain examples should not be restrictive of further possible examples.

20

Throughout the description of the figures same or similar reference numerals refer to same or similar elements and/or features, which may be identical or implemented in a modified form while providing the same or a similar function. The thickness of lines, layers and/or areas in the figures may also be exaggerated for clarification.

25

When two elements A and B are combined using an “or”, this is to be understood as disclosing all possible combinations, i.e., only A, only B as well as A and B, unless expressly defined otherwise in the individual case. As an alternative wording for the same combinations, "at least one of A and B" or "A and/or B" may be used. This applies equivalently to combinations of more than two elements.

30

If a singular form, such as “a”, “an” and “the” is used and the use of only a single element is not defined as mandatory either explicitly or implicitly, further examples may also use several

elements to implement the same function. If a function is described below as implemented using multiple elements, further examples may implement the same function using a single element or a single processing entity. It is further understood that the terms "include", "including", "comprise" and/or "comprising", when used, describe the presence of the specified features, integers, steps, operations, processes, elements, components and/or a group thereof, but do not exclude the presence or addition of one or more other features, integers, steps, operations, processes, elements, components and/or a group thereof.

Fig. 1a shows a block diagram of an example of an authentication device 10. The authentication device 10 comprises an interface 12 and processing circuitry 14. Optionally, the authentication device 10 further comprises a storage device 16. The processing circuitry 14 is coupled with the interface 12 and with the optional storage device 16. In general, the functionality of the authentication device 10 is provided by the processing circuitry 14, in conjunction with the interface 12 (for communicating with other devices, e.g., with a further device 5, and/or with a device comprising the authentication device) and/or the optional storage device 16 (for storing and/or retrieving information).

The processing circuitry is configured to obtain authentication information from the further device 5. The authentication information comprises information for identifying a non-fungible token linked to an authentication identity of an owner of the further device 5. The processing circuitry is configured to authenticate the further device 5 vis-à-vis the authentication device 10 based on the information for identifying the non-fungible token.

Fig. 1a further shows a system comprising the authentication device 10 and the further device 5.

Fig. 1b shows a flow chart of an example of a corresponding authentication method. The authentication method comprises obtaining 130 the authentication information from the (further) device. The authentication information comprises the information for identifying the non-fungible token linked to an authentication identity of an owner of the (further) device. The authentication method comprises authenticating 170 the (further) device based on the information for identifying the non-fungible token. For example, the authentication method may be performed by the authentication device or by another device or service, such as a machine, a web server or web service.

The proposed concept relates to an authentication device, to a corresponding authentication method, and to a corresponding authentication computer program. In the following, the proposed concept will be introduced in more detail with respect to the authentication device.

5 Features introduced in connection with the authentication device may likewise be included in the corresponding authentication method and authentication computer program.

The proposed concept relates to the authentication of the further device vis-à-vis the authentication device, or rather vis-à-vis a device comprising the authentication device. For example, 10 the proposed concept may be used to authenticate the further device vis-a-vis a web server (200 shown in Fig. 2), e.g., to log the further device into the owner's use account (i.e., into a user account associated with the authentication identity of the owner) on a web site or in an application. Various examples of the present disclosure may thus relate to a concept for using NFTs for password-less login, e.g., on multiple internet-based services. This scenario is 15 shown in Fig. 2, for example. In this case, the authentication device 10 may be part of the web server 200, or a web service (e.g., such as a file synchronization service, a social media service, or a messaging service) may perform the authentication method. However, the same concept is also applicable to other authentication scenarios. For example, the proposed concept may be used to authenticate the owner vis-a-vis a machine (300, as shown in Fig. 3), 20 such as a transportation device or a self-service vending device. Accordingly, as shown in Fig. 3, the machine may comprise the authentication device, or be configured to perform the authentication method. In this scenario, the owner may authenticate vis-à-vis a rental transportation device, such as a rental scooter, rental bike, or rental car, or vis-à-vis a public transportation vehicle, such as a bus, a train, a subway car, or a tram. Likewise, the owner may 25 authenticate vis-a-vis a self-service vending device, such as a turnstile (for accessing public transportation or a paid venue), a ticket machine, or a snack or drink vending machine etc. However, the proposed concept is not limited to such scenarios. For example, the proposed concept may also be used to authenticate vis-à-vis a bank or government agency.

30 In the proposed concept, the further device 5 interacts with the authentication device 10. The further device 5 is a device that is owned by (or at least in rightful possession of) the aforementioned owner and is used by the owner to communicate with the authentication device. In this context, the term "owner of the further device" refers to a person (or organization) that owns or is in rightful possession of the further device. For example, the further device 5 may

be a smart device, such as a smartphone or smartwatch being used by the owner of the further device. Alternatively, the further device 5 may be a hardware wallet, or a computer, such as a tablet computer, laptop computer or desktop computer.

- 5 Communication between the further device 5 and the authentication device 10 may occur via various channels. In general, at least a portion of the communication between the further device 5 and the authentication device 10 may occur via a computer network, e.g., via the internet, via a local network, or via an ad-hoc network established via WiFi, Near-Field-Communication (NFC), Bluetooth or the like. Some of the communication may be performed out-of-
- 10 band. For example, the authentication device may be configured to perform some communication by displaying the information, e.g., as two-dimensional visual code (such as a so-called Quick Response, QR, code) on a display or on a website. For example, such information may be shown on a display of the transportation device or self-service vending machine, or on a website. For example, to login into a user account of a website from a computer, a two-dimensional code may be shown on the website displayed by the computer, which may be
- 15 scanned by a smartphone or tablet computer, with the authentication process being performed by the smartphone or tablet computer and the authentication device, but the authentication having the effect of performing the login on the computer.
- 20 In the following, the focus is on the use case of authenticating vis-à-vis a web server or web service, e.g., to log into a user account on a website or to log in an application into a user account on a web service.

In a nutshell, the proposed concept uses the ownership of an NFT, and its link to the authentication identity of the owner of the further device, to authenticate the further device vis-à-vis the authentication device. The further device provides the authentication information to the authentication device, with the authentication information including a reference to the NFT, and the authentication device authenticates the further device based on said authentication information.

30

In the following, various optional aspects of the proposed authentication concept are introduced in connection with Fig. 1b. While Fig. 1b is primarily used to illustrate the authentication method, it, more generally, includes an overview of the tasks potentially performed by the authentication device 10 and/or by the further device 5. In the Figures, and in particular

in Fig. 1b, optional components or tasks are marked with dashed lines. While Fig. 1b implies an order in which the respective actions are taken, this order represents merely an example. For example, at least some of the authentication information may be obtained 130 before challenge information is provided 110 to the further device, or the authentication information may be verified 150 after a link between the non-fungible token and the authentication identity is verified 160.

As shown in Fig. 1b, in some examples, the processing circuitry may be configured to provide challenge information to the further device. Accordingly, the authentication method may comprise providing 110 the challenge information to the (further) device. This challenge information has the purpose of making each authentication process unique, e.g., to thwart replay attacks and/or to distinguish different authentication processes. Accordingly, the challenge information may be unique, i.e., different for every authentication process. IN other words, the challenge information may comprise a unique one-time code. In addition, the challenge information may comprise information on a destination of the authentication information, e.g., on how to provide the authentication information to the authentication device. For example, the processing circuitry may be configured to generate a new challenge information for each authentication process (e.g., for each time the challenge information is shown on a website or otherwise transmitted to the further device, and/or to generate a new challenge information according to a pre-defined schedule (e.g., if the challenge information is shown on a display of the device comprising the authentication device).

As outlined above, the challenge information may be shown on a web site or a display of a device comprising the authentication device. For example, the processing circuitry may be configured to provide the challenge information to the further device as a two-dimensional visual code (e.g., a QR code), e.g., a two-dimensional visual code being displayed on a display device. For example, the two-dimensional visual code may be scanned by the further device to obtain the respective information. Alternatively, the processing circuitry may be configured to provide the challenge information to the further device via a computer network (e.g., via the interface 12, and the internet, a local network, or an ad-hoc network), e.g., as binary information or as two-dimensional visual code shown on a website. The further device 5 may then generate the authentication information based on the challenge information. In other words, the authentication information may be based on the challenge information and/or received in response to the challenge information.

In some examples of the proposed concept, cryptography may be used to provide additional security to the authentication process. In particular, some properties on how non-fungible tokens are stored in cryptocurrency wallets may be used to provide additional security to the authentication process. In the following, a short introduction is given on the mechanics behind non-fungible tokens.

In general, a non-fungible token (NFT), e.g., an Ethereum-based non-fungible token, is based on a smart contract that manages ownership of the non-fungible token. An NFT can only have one owner at a time. In particular, every NFT might have an owner, with the ownership being on public record and easy for anyone to verify. For example, every NFT may have an owner, a creator, and a history (which are denoted “provenance”), which are verifiable on the distributed ledger. For example, an Ethereum NFT may be associated with information such as a contract address, token identifier, token standard (such as ERC-721, a standard related to the Ethereum blockchain), and metadata. For example, ownership may be managed through a unique identifier (denoted uniqueID) and metadata that no other token can replicate. NFTs may be minted through so-called smart contracts, which are computer programs or set of instructions stored on a blockchain, that can be used assign ownership and manage the transferability of the NFTs. When someone creates or mints an NFT, they may execute code stored in smart contracts that conform to different standards, such as ERC-721. This information may be added to the distributed ledger where the NFT is being managed. The minting process, from a high level, may comprise the following tasks: Creating a new block, validating information, and recording information into the blockchain.

In general, NFTs on the Ethereum blockchain have some special properties. NFTs are, in general, not directly interchangeable with other tokens 1:1. For example 1 ETH (Ethereum currency unit) is exactly the same as another ETH. This is not the case with NFTs. Ethereum NFTs live on Ethereum and can be bought and sold on any Ethereum-based NFT market.

For example, each NFT minted has a unique identifier that is directly linked to one Ethereum address. Each NFT also has an owner, with the owner being easily verifiable. In particular, the owner of an NFT can easily prove that they own the NFT. Proving someone owns an NFT is very similar to proving to have ETH in someone’s account. For example, if someone purchases an NFT, the ownership of the unique token is transferred to that someone’s wallet via

their public address. The token proves that their copy of the digital file is the original. In particular, the private key of the NFTs owner is proof-of-ownership of the original. For example, ownership of the NFT can be proven by signing messages to prove that the owner owns the private key behind the address. This provides prove for other users of the blockchain that the private keys behind that address control the NFT. In effect, a signed message can be used as proof that someone owns the private keys without revealing them to anybody and thus proving they own the NFT as well. For example, a public key can be derived from a cryptocurrency address (only) if a transaction has been sent from the address. Ethereum addresses are generated as follows: Start with the public key (64 bytes) and calculate the Keccak-256 hash of the public key, resulting in a string that is 32 bytes. (SHA3-256 eventually became the standard, but Ethereum uses Keccak). The last 20 bytes (or 40 characters) of this public key are used as address (Keccak-256). Or, in other words, the first 12 bytes may be used. These 20 bytes are the address, or 40 characters. When prefixed with 0x, the address becomes 42 characters long.

15

The content creator's public key serves as a certificate of authenticity for that particular digital artefact. The creator's public key is essentially a permanent part of the token's history. The creator's public key can demonstrate that the token the buyer holds was created by a particular individual, thus contributing to its market value (proving the token is not counterfeit).

20

When a NFT is bought, in effect, the right to transfer the token to the buyer's digital wallet is bought. The token proves that the buyer's copy of a digital file is the original, like owning an original painting. And just as paintings can be copied and distributed as inexpensive posters, anyone can have a digital copy of an NFT. However, the buyer's private crypto key can be used as proof of ownership of the original. The content creator's public crypto key, on the other hand, can serve as the certificate of authenticity for that particular digital artifact. This pair of the creator's public key and the owner's private key may primarily determine the value of any NFT token.

30

In the proposed concept, two of the aforementioned concepts are used for the authentication process – that the address the non-fungible token is stored at is derived from the public key of the owner of the non-fungible token, and that the owner can prove ownership of the non-fungible token by signing (i.e., by creating a cryptographic signature) using the corresponding private key. In the following, where the term public key and private key (of the owner) are

used, this refers to the public and private key of the cryptocurrency wallet, i.e., the private key being used to sign transactions on the distributed ledger, and the public key from which the address on the distributed ledger is derived. In the following, the public key is also referred to as “cryptographic key”, and the signature being generated using the private key is also referred to as “cryptographic signature”.

In various examples of the proposed concept, the challenge information is processed by the further device, and (at least a portion of) the authentication information is generated and provided based on the challenge information. In particular, the aforementioned cryptographic signature may be generated, by the further device, based on at least a portion of the challenge information, e.g., using the aforementioned private key of the owner. Accordingly, the authentication information may further comprise the cryptographic signature, with the cryptographic signature being generated 120 (as further shown in Fig. 1b) based on the challenge information (and based on the private key of the owner). For example, the further device may generate 120 the cryptographic signature based on the challenge information.

The cryptographic signature may be included in the authentication information alongside (i.e., in the same message), or separate from (i.e., in a different message), the information for identifying the non-fungible token linked to the authentication identity of an owner of the further device. For example, the information for identifying a non-fungible token may be an address of the non-fungible token on a distributed ledger, or an identifier of the non-fungible token (which may be used, by the authentication device, to look up the address of the non-fungible token on the distributed ledger).

In the basic implementation of the proposed concept, the authentication information is primarily used for identifying the non-fungible token, and thus an authentication identity (e.g., user account, customer identify etc.) of the owner of the further device (and non-fungible token). In the proposed concept, ownership (including rightful possession) of the further device and of the non-fungible token are linked and can be proven by the further device providing the cryptographic signature. Another link exists between the authentication identity of the owner of the further device and the non-fungible token. For example, the authentication identity (e.g., user account, customer identify etc.) of the owner of the further device may comprise a reference to the non-fungible token and may be linked with the non-fungible token by the reference.

When the owner of the further device initiates the authentication process, the authentication information is provided to instruct the authentication device to authenticate the authentication identity linked with the non-fungible token identified by the authentication information. The processing circuitry may be configured to determine the authentication identity of the owner of the further device based on the authentication information (e.g., to look up the authentication identity of the owner based on the non-fungible token identified by the authentication information). To make sure that the owner of the further device is also the owner of the non-fungible token, the cryptographic signature may be provided, which enables verification of the link between the owner of the further device and the non-fungible token. For example, the processing circuitry being configured to verify the cryptographic signature based on the information for identifying the non-fungible token, with the authentication being successful if the verification of the cryptographic signature is successful.

To verify the cryptographic signature, a mechanism commonly used in public private key authentication may be used. The authentication device may comprise, e.g., stored by the storage device 12, a cryptographic key that is suitable for verifying the cryptographic signature included in the authentication information. For example, the processing circuitry may be configured to use the information for identifying the non-fungible token to obtain the cryptographic key linked to the authentication identity of the owner of the further device. Accordingly, as further shown in Fig. 1b, the authentication method may comprise obtaining the cryptographic key using the information for identifying the non-fungible token. For example, the information for identifying the non-fungible token may be used to look up the cryptographic key. For example, the information for identifying the non-fungible token may be used to obtain (e.g., load) the cryptographic key from the storage device of the authentication device, or to request and download the cryptographic key from a remote server associated with the authentication device. Accordingly, the processing circuitry is configured to obtain (e.g., load) the cryptographic key from a storage device of the authentication device, or to request and download the cryptographic key from the remote server. For example, the cryptographic key may have been provided as part of a registration process for creating the authentication identity and stored in the storage device or remote server. For example, the remote server-based approach may be used in scenarios where a plurality of authentication devices (e.g., that are part of a plurality of machines, such as rental vehicles or self-service vending devices) use the same authentication identity.

The cryptographic key may then be used to verify one or both of a) the cryptographic signature and the link between the non-fungible token and b) the authentication identity. In effect, the processing circuitry may be configured to authenticate the further device based on the cryptographic key. For example, the processing circuitry may be configured to verify the cryptographic signature that is part of the authentication information using the cryptographic key, with the authentication being successful if the verification of the cryptographic signature is successful. As mentioned above, public private key authentication may be used for this purpose, e.g., to verify, using the public key (i.e., the cryptographic key) to verify that the cryptographic signature was generated using the corresponding private key. In other words, the cryptographic key may be the public key of the key pair of the owner of the further device, and the authentication may be successful if the cryptographic signature is generated using the private key of the key pair. Accordingly, the authentication method comprise verifying the cryptographic signature (and thus the authentication information) using the cryptographic key.

As mentioned above, the cryptographic key may also be used to verify the link between the non-fungible token and the authentication identity (and thus the user). In other words, the processing circuitry may be configured to verify the link between the non-fungible token and the authentication identity using the cryptographic key. Accordingly, as further shown in Fig. 1b, the authentication method may comprise verifying the link between the non-fungible token and the authentication identity using the cryptographic key. In this context, the term “verifying the link between the non-fungible token and the authentication identity” means that the non-fungible token is indeed linked to an address on the distributed ledger that is associated with the owner, and thus also the identification identity of the owner. In other words, the processing circuitry may be configured to verify the link between the non-fungible token and the authentication identity based on the address of the non-fungible token on the distributed ledger. If the link is intact, this address is derivable from the cryptographic key. In other words, the address of the non-fungible token on the distributed ledger is derivable from the cryptographic key (as long as the link between the non-fungible token and the authentication identity is intact). To verify the link, the address of the non-fungible token may be compared with an address derived from the cryptographic key. For example, as outlined above, in Ethereum, the address can be derived from the public key by calculating the Keccak-256 hash

of the public key and taking the last 20 bytes (or 40 characters) of the resulting hash, and prefixing "0x". If the addresses match, the verification of the link may be deemed successful.

5 The authentication device's purpose is to authenticate the further device vis-à-vis the authentication device based on the information for identifying the non-fungible token. In the most basic implementation, the link between the non-fungible token and the authentication identity of the owner may be used to authenticate the further device vis-à-vis the authentication device. To increase security, the aforementioned verification or verifications may be carried out. For example, the authentication may be successful if the cryptographic signature can be verified,
10 e.g., if the cryptographic signature is generated using a private key of the key pair of the owner, and/or if the link between the non-fungible token and the authentication identify can be verified, e.g., if the address of the non-fungible token is derivable from the cryptographic key.

15 If the authentication is successful, the owner may be logged into the user profile on the web site, a rental may be started of the rental vehicle, a trip may be started on public transportation, or a sale of a good or service may be performed by the self-service vending machine. To this effect, the authentication device may be configured to provide a signal or message indicating that the authentication was successful (or that authentication has been unsuccessful), e.g., to
20 the device comprising the authentication device. As a result, the owner may be logged into their user account on the further device (or another device, if the further device is used to aid login on another device), or the respective rental, admittance to public transportation or sale of a good or service may be performed by the respective device comprising the authentication device.

25 In the following, a short introduction is given with respect to an initial registration of the authentication identity at the authentication device. Fig. 1c shows a flow chart of an example of a registration method for initial registration prior to authentication. For example, the registration method may be performed by the authentication device. As is evident, the registration process is similar to the authentication process. As part of the registration, the processing
30 circuitry may be configured to provide 101 challenge information to the further device. Accordingly, the registration method may comprise providing 101 the challenge information to the further device. The further device may generate 102 the cryptographic signature, and the processing circuitry may be configured to obtain registration information (which may be

similar to the authentication information) comprising the cryptographic signature, the information for identifying the non-fungible token, and the cryptographic key from the further device. Accordingly, the registration method may comprise obtaining 103 the registration information. In effect, the processing circuitry may be configured to obtain the cryptographic key from a device of the owner of the further device (e.g., from the further device or from another device of the owner) during registration of the authentication identity at the authentication device, and to store the cryptographic key using the storage device. The processing circuitry may then be configured to verify the registration information (which may be implemented similar to the verification of the authentication information) and/or to verify the link between the non-fungible token and the authentication identity based on the cryptographic provided during the registration. Accordingly, the registration method may comprise verifying 104 the registration information and/or verifying 105 the link between the non-fungible token and the authentication identity. Finally, the processing circuitry may be configured to store the cryptographic key, e.g., if one or both verifications are successful. Accordingly, the registration method may comprise storing 106 the cryptographic key.

For example, the interface 12 may correspond to one or more inputs and/or outputs for receiving and/or transmitting information, which may be in digital (bit) values according to a specified code, within a module, between modules or between modules of different entities. For example, the interface 12 may comprise interface circuitry configured to receive and/or transmit information.

The processing circuitry 14 may be implemented using one or more processing units, one or more processing devices, any means for processing, such as a processor, a computer or a programmable hardware component being operable with accordingly adapted software. In other words, the described function of the processing circuitry 14 may as well be implemented in software, which is then executed on one or more programmable hardware components. Such hardware components may comprise a general-purpose processor, a Digital Signal Processor (DSP), a micro-controller, etc.

For example, the storage device 16 may comprise at least one element of the group of a computer readable storage medium, such as a magnetic or optical storage medium, e.g., a hard disk drive, a flash memory, Floppy-Disk, Random Access Memory (RAM), Programmable

Read Only Memory (PROM), Erasable Programmable Read Only Memory (EPROM), an Electronically Erasable Programmable Read Only Memory (EEPROM), or a network storage.

5 More details and aspects of the authentication device, authentication method, authentication computer program, registration method, a corresponding registration computer program and of the devices, machines or services comprising the authentication device or performing the authentication method or registration method are mentioned in connection with the proposed concept or one or more examples described above or below (e.g., Fig. 2 to 4). The authentication device, authentication method, authentication computer program, registration method,
10 registration computer program and the devices, machines or services comprising the authentication device or performing the authentication method or registration method may comprise one or more additional optional features corresponding to one or more aspects of the proposed concept, or one or more examples described above or below.

15 In the following, some figures are provided with respect to devices or services that may employ the proposed authentication approach. Fig. 2 shows a block diagram of an example of a web server 200 comprising the authentication device 10 (e.g., as introduced in connection with Figs. 1a to 1c). Similarly, the web server, or more generally a web service, may perform the authentication method (and/or the registration method) introduced in connection with
20 Figs. 1b and 1c. For example, the authentication device may be used to log in the owner on a web site or to log in an application on the further device (denoted “client device” 5 in Fig. 2, as the counterpart of a server is a client).

In some examples, as shown in Fig. 3, the authentication device may be used to authenticate
25 the owner, via their device, vis-à-vis a machine, such as a transportation device or a self-service vending device. In Fig. 3, an example is shown where the machine is a rental scooter, which comprises the authentication device. Fig. 3 shows a schematic diagram of an example of a rental scooter comprising the authentication device 10 (e.g., as introduced in connection with Figs. 1a to 1c). For example, the authentication device may be used to authenticate the
30 owner vis-à-vis the rental scooter, e.g., to start a rental process. In Fig. 3, the further device is a smart device 5, such as a smartphone or smartwatch.

More details and aspects of the web server, the machine/scooter, the authentication device, and the client device/further device are mentioned in connection with the proposed concept

or, one or more examples described above or below (e.g., Figs. 1a to 1c, 4). The web server, the machine/scooter, the authentication device, and the client device/further device may comprise one or more additional optional features corresponding to one or more aspects of the proposed concept or, one or more examples described above or below.

5

As shown in connection with Figs. 1a to 1c, registering a user on a website or internet service using an NFT can be done by presenting the NFT cryptocurrency address, or the unique identifier of the NFT, together with the public key of the cryptocurrency address from which it was derived. During the registration process, the user may provide a one-time signature to the website or internet-based service proving that the user is indeed the owner of the NFT. The data to sign can be offered as a unique one-time QR code.

10

Later on, the authentication of the user on a website or internet service may be done by providing the NFT crypto address together with a new one-time signature proving that the user is the owner of the registered NFT. Again, the data to sign can be offered as a unique one-time QR code. In both registration and authentication, the website or internet service can verify the signature using the stored public key and cryptographic address for the NFT. In general, only the holder of the NFT has the private key that matches the public key that generated the cryptocurrency address holding the NFT token.

15

20

Fig. 4 shows a diagram of an example of actions used to register or authenticate a user on a website or internet-based service using an NFT. In the example shown in Fig. 4, a website 420 shows a unique one-time code to sign as a QR code (1). A user 410 scans the QR code to obtain the unique code and signs it with his private key 430 (2). The user sends a signature, public key 440 and NFT crypto address 450 (of NFT 460) (3). An NFT lookup is done if the crypto address 450 holds a valid NFT token 460. After validating the signature, the public key and crypto address is stored (4) in a database 480 of the web server / service backend 470. A valid signature proves that the signer holds the private key that matches the public key from which the crypto address that holds the NFT is derived. As shown in Fig. 4, the public key 440 is derived from the private key 430 through an algorithmic transformation, and the crypto address 450 holding the NFT token is derived from the public key 440 through a hash function.

25

30

- In the following, the actions taken to authenticate (login) a user on a website or internet-based service using an NFT are shown, which is similar to the registration process. (1) The website 420 shows a unique one-time code to sign as a QR code. (2) The user 410 scans the QR code to obtain the unique code and signs it with his private key. (3) The user 410 sends a signature and NFT crypto address 450 (or identifier) to the web server 470. (4) The crypto address is used to look up the public key in the database 480. (5) After validating the signature, the user 410 is granted access (logged in) (as a valid signature proves that the signer holds the private key that matches the public key from which the crypto address that holds the NFT is derived).
- 10 In the proposed concept, anyone trying to authenticate by simply providing an already registered NFT crypto address may fail because no valid signature can be provided. For example, if the token to sign is a one-time unique token, providing an intercepted signature might not be an option.
- 15 When the NFT is sold, the token is transferred to the cryptocurrency address of the buyer who now becomes the new owner. The new cryptocurrency address also has a new public and private key. This automatically ends NFT authentication for the previous owner.

Various examples provide an authentication using an NFT, e.g., by using a signature made by the private key that matches the public key that is used to derive the crypto address holding the NFT token.

In the proposed concept, the NFT may be thought of as a verifiable credential. In general, a verifiable credential may represent (all of) the same information that a physical credential represents. The addition of technologies, such as digital signatures, may make verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. Holders of verifiable credentials may generate so-called verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics. A credential or presentation may be considered to be verifiable if at least one proof mechanism, and the details necessary to evaluate that proof, is defined (i.e., expressed) for the credential or presentation to be a verifiable credential or verifiable presentation.

More details and aspects of the NFT-based authentication approach are mentioned in connection with the proposed concept, or one or more examples described above or below (e.g., Figs.

1a to 3). The NFT-based authentication approach may comprise one or more additional optional features corresponding to one or more aspects of the proposed concept, or one or more examples described above or below.

5 In the following, some examples of the proposed concept are given:

(1) An authentication device comprising:

an interface for communicating with a further device (5);

10

processing circuitry configured to:

obtain authentication information from the further device, the authentication information comprising information for identifying a non-fungible token linked to an authentication identity of an owner of the further device; and

15

authenticate the further device vis-à-vis the authentication device based on the information for identifying the non-fungible token.

(2) The authentication device according to (1), wherein the authentication information further comprises a cryptographic signature, the processing circuitry being configured to verify the cryptographic signature based on the information for identifying the non-fungible token, with the authentication being successful if the verification of the cryptographic signature is successful.

20

(3) The authentication device according to (2), wherein the processing circuitry is configured to provide challenge information to the further device, with the cryptographic signature being generated based on the challenge information.

25

(4) The authentication device according to (3), wherein the processing circuitry is configured to provide the challenge information to the further device via a computer network.

30

(5) The authentication device according to (3), wherein the processing circuitry is configured to provide the challenge information to the further device as a two-dimensional visual code being displayed on a display device.

- (6) The authentication device according to one of (3) to (5), wherein the challenge information comprises a unique one-time code.
- 5 (7) The authentication device according to one of (1) to (6), wherein the processing circuitry is configured to use the information for identifying the non-fungible token to obtain a cryptographic key linked to the authentication identity of the owner of the further device, and to authenticate the further device based on the cryptographic key.
- 10 (8) The authentication device according to (7), wherein the processing circuitry is configured to obtain the cryptographic key from a storage device of the authentication device.
- 15 (9) The authentication device according to one of (7) or (8), wherein the processing circuitry is configured to obtain the cryptographic key from a device of the owner of the further device during registration of the authentication identity at the authentication device, and to store the cryptographic key using the storage device.
- 20 (10) The authentication device according to one of (7) to (9), wherein the processing circuitry is configured to verify a link between the non-fungible token and the authentication identity using the cryptographic key.
- 25 (11) The authentication device according to (10), wherein the processing circuitry is configured to verify the link between the non-fungible token and the authentication identity based on an address of the non-fungible token on a distributed ledger, with the authentication being successful if the address of the non-fungible token is derivable from the cryptographic key.
- 30 (12) The authentication device according to one of (7) to (11), wherein the processing circuitry is configured to verify a cryptographic signature that is part of the authentication information using the cryptographic key, with the authentication being successful if the verification of the cryptographic signature is successful.

(13) The authentication device according to (12), wherein the cryptographic key is a public key of a key pair of the owner of the further device, with the authentication being successful if the cryptographic signature is generated using a private key of the key pair.

5

(14) The authentication device according to one of (7) to (13), wherein an address of the non-fungible token on a distributed ledger is derivable from the cryptographic key.

10

(15) The authentication device according to one of (1) to (14), wherein the information for identifying a non-fungible token is an address of the non-fungible token on a distributed ledger.

15

(16) The authentication device according to one of (1) to (15), wherein the information for identifying a non-fungible token is an identifier of the non-fungible token.

(17) A web server comprising the authentication device according to one of (1) to (16).

20

(18) A machine comprising the authentication device according to one of (1) to (17).

(19) The machine according to (18), wherein the machine is a transportation device or a self-service vending device.

25

(20) An authentication method comprising:

obtaining authentication information from a device, the authentication information comprising information for identifying a non-fungible token linked to an authentication identity of an owner of the device; and

30

authenticating the device based on the information for identifying the non-fungible token.

(21) A web service performing the authentication method according to (20).

(22) A computer program having a program code for performing the method of (20) when the computer program is executed on a computer, a processor, or a programmable hardware component.

5

10

The aspects and features described in relation to a particular one of the previous examples may also be combined with one or more of the further examples to replace an identical or similar feature of that further example or to additionally introduce the features into the further example.

15

20

25

Examples may further be or relate to a (computer) program including a program code to execute one or more of the above methods when the program is executed on a computer, processor, or other programmable hardware component. Thus, steps, operations, or processes of different ones of the methods described above may also be executed by programmed computers, processors, or other programmable hardware components. Examples may also cover program storage devices, such as digital data storage media, which are machine-, processor- or computer-readable and encode and/or contain machine-executable, processor-executable or computer-executable programs and instructions. Program storage devices may include or be digital storage devices, magnetic storage media such as magnetic disks and magnetic tapes, hard disk drives, or optically readable digital data storage media, for example. Other examples may also include computers, processors, control units, (field) programmable logic arrays ((F)PLAs), (field) programmable gate arrays ((F)PGAs), graphics processor units (GPU), application-specific integrated circuits (ASICs), integrated circuits (ICs) or system-on-a-chip (SoCs) systems programmed to execute the steps of the methods described above.

30

It is further understood that the disclosure of several steps, processes, operations, or functions disclosed in the description or claims shall not be construed to imply that these operations are necessarily dependent on the order described, unless explicitly stated in the individual case or necessary for technical reasons. Therefore, the previous description does not limit the execution of several steps or functions to a certain order. Furthermore, in further examples, a single step, function, process, or operation may include and/or be broken up into several sub-steps, -functions, -processes or -operations.

If some aspects have been described in relation to a device or system, these aspects should also be understood as a description of the corresponding method. For example, a block, device or functional aspect of the device or system may correspond to a feature, such as a method step, of the corresponding method. Accordingly, aspects described in relation to a method
5 shall also be understood as a description of a corresponding block, a corresponding element, a property or a functional feature of a corresponding device or a corresponding system.

The following claims are hereby incorporated in the detailed description, wherein each claim may stand on its own as a separate example. It should also be noted that although in the claims
10 a dependent claim refers to a particular combination with one or more other claims, other examples may also include a combination of the dependent claim with the subject matter of any other dependent or independent claim. Such combinations are hereby explicitly proposed, unless it is stated in the individual case that a particular combination is not intended. Furthermore, features of a claim should also be included for any other independent claim, even if that
15 claim is not directly defined as dependent on that other independent claim.

Claims

What is claimed is:

- 5 1. An authentication device comprising:

an interface for communicating with a further device;

processing circuitry configured to:
10 obtain authentication information from the further device, the authentication information comprising information for identifying a non-fungible token linked to an authentication identity of an owner of the further device; and
authenticate the further device vis-à-vis the authentication device based on the information for identifying the non-fungible token.
15
2. The authentication device according to claim 1, wherein the authentication information further comprises a cryptographic signature, the processing circuitry being configured to verify the cryptographic signature based on the information for identifying the non-fungible token, with the authentication being successful if the verification of the cryptographic signature is successful.
20
3. The authentication device according to claim 2, wherein the processing circuitry is configured to provide challenge information to the further device, with the cryptographic signature being generated based on the challenge information.
25
4. The authentication device according to claim 3, wherein the processing circuitry is configured to provide the challenge information to the further device via a computer network.
- 30 5. The authentication device according to claim 3, wherein the processing circuitry is configured to provide the challenge information to the further device as a two-dimensional visual code being displayed on a display device.

6. The authentication device according to claim 3, wherein the challenge information comprises a unique one-time code.
- 5 7. The authentication device according to claim 1, wherein the processing circuitry is configured to use the information for identifying the non-fungible token to obtain a cryptographic key linked to the authentication identity of the owner of the further device, and to authenticate the further device based on the cryptographic key.
- 10 8. The authentication device according to claim 7, wherein the processing circuitry is configured to obtain the cryptographic key from a device of the owner of the further device during registration of the authentication identity at the authentication device, and to store the cryptographic key using the storage device.
- 15 9. The authentication device according to claim 7, wherein the processing circuitry is configured to verify a link between the non-fungible token and the authentication identity using the cryptographic key.
- 20 10. The authentication device according to claim 9, wherein the processing circuitry is configured to verify the link between the non-fungible token and the authentication identity based on an address of the non-fungible token on a distributed ledger, with the authentication being successful if the address of the non-fungible token is derivable from the cryptographic key.
- 25 11. The authentication device according to claim 7, wherein the processing circuitry is configured to verify a cryptographic signature that is part of the authentication information using the cryptographic key, with the authentication being successful if the verification of the cryptographic signature is successful.
- 30 12. The authentication device according to claim 11, wherein the cryptographic key is a public key of a key pair of the owner of the further device, with the authentication being successful if the cryptographic signature is generated using a private key of the key pair.

13. The authentication device according to claim 12, wherein an address of the non-fungible token on a distributed ledger is derivable from the cryptographic key.

14. The authentication device according to claim 1, wherein the information for identifying a non-fungible token is an address of the non-fungible token on a distributed ledger, or wherein the information for identifying a non-fungible token is an identifier of the non-fungible token.

15. A web server comprising the authentication device according to claim 1.

16. A machine comprising the authentication device according to claim 1.

17. The machine according to claim 16, wherein the machine is a transportation device or a self-service vending device.

18. An authentication method comprising:

obtaining authentication information from a device, the authentication information comprising information for identifying a non-fungible token linked to an authentication identity of an owner of the device; and

authenticating the device based on the information for identifying the non-fungible token.

19. A web service performing the authentication method according to claim 18.

20. A computer program having a program code for performing the method of claim 18, when the computer program is executed on a computer, a processor, or a programmable hardware component.

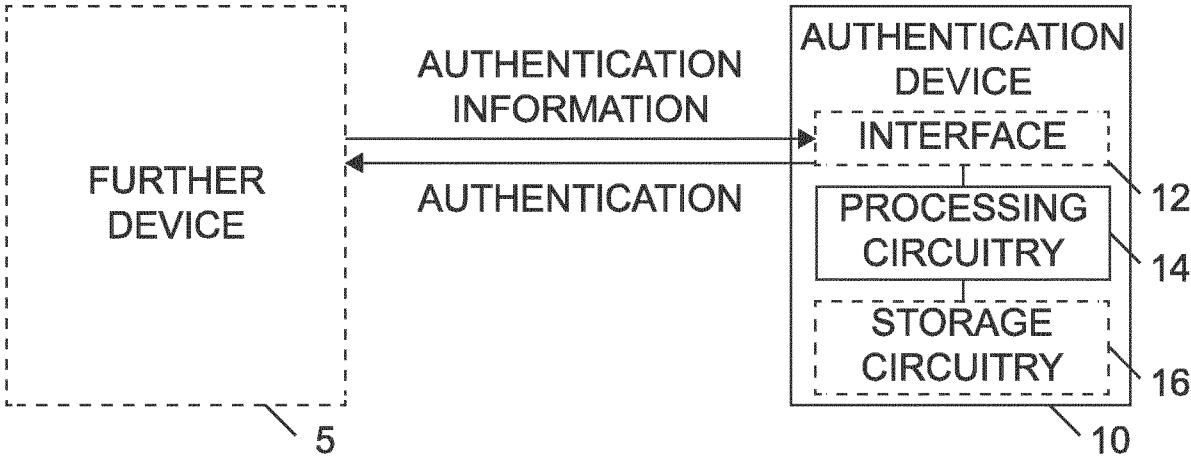


Fig. 1a

2 / 6

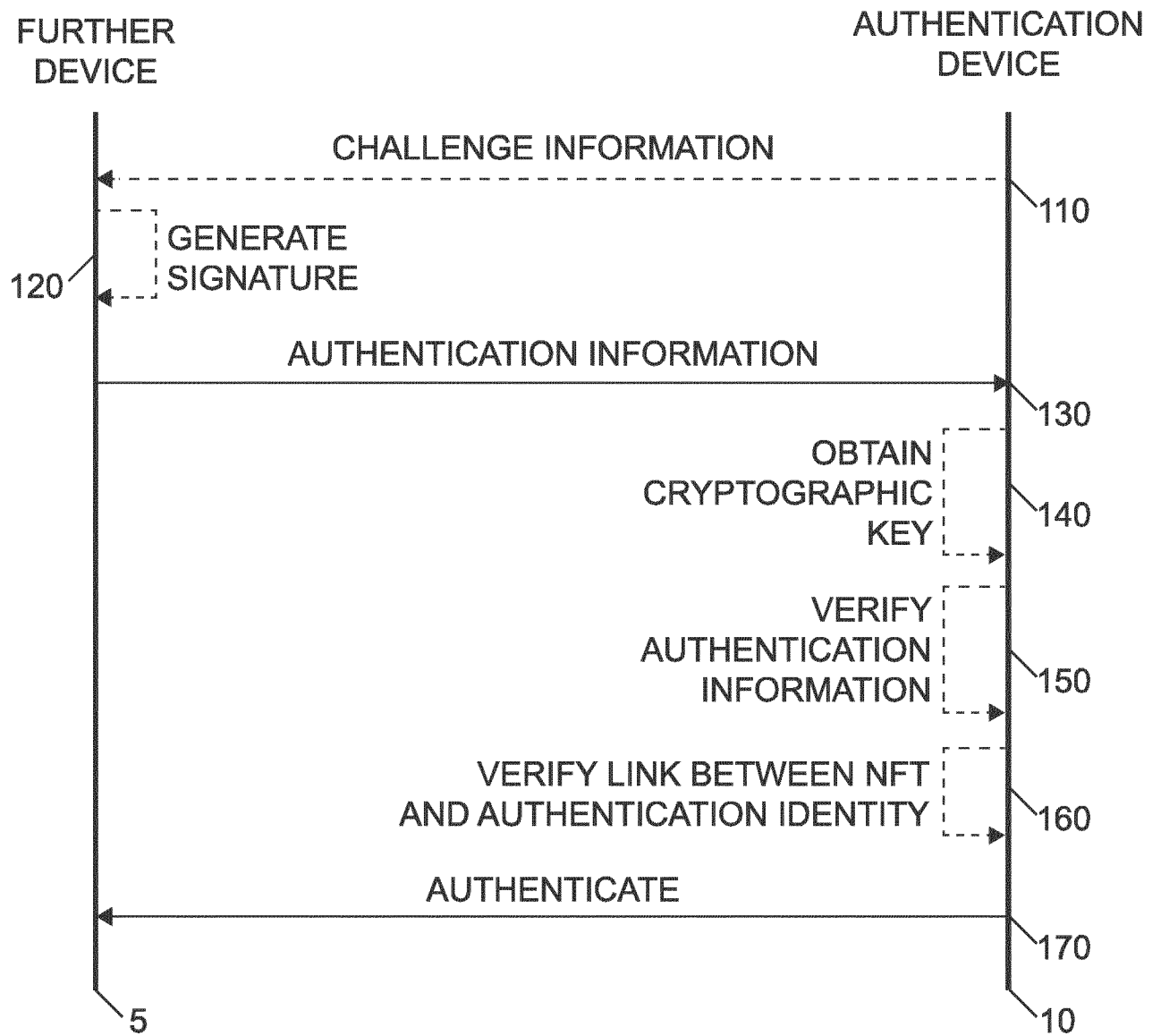


Fig. 1b

3 / 6

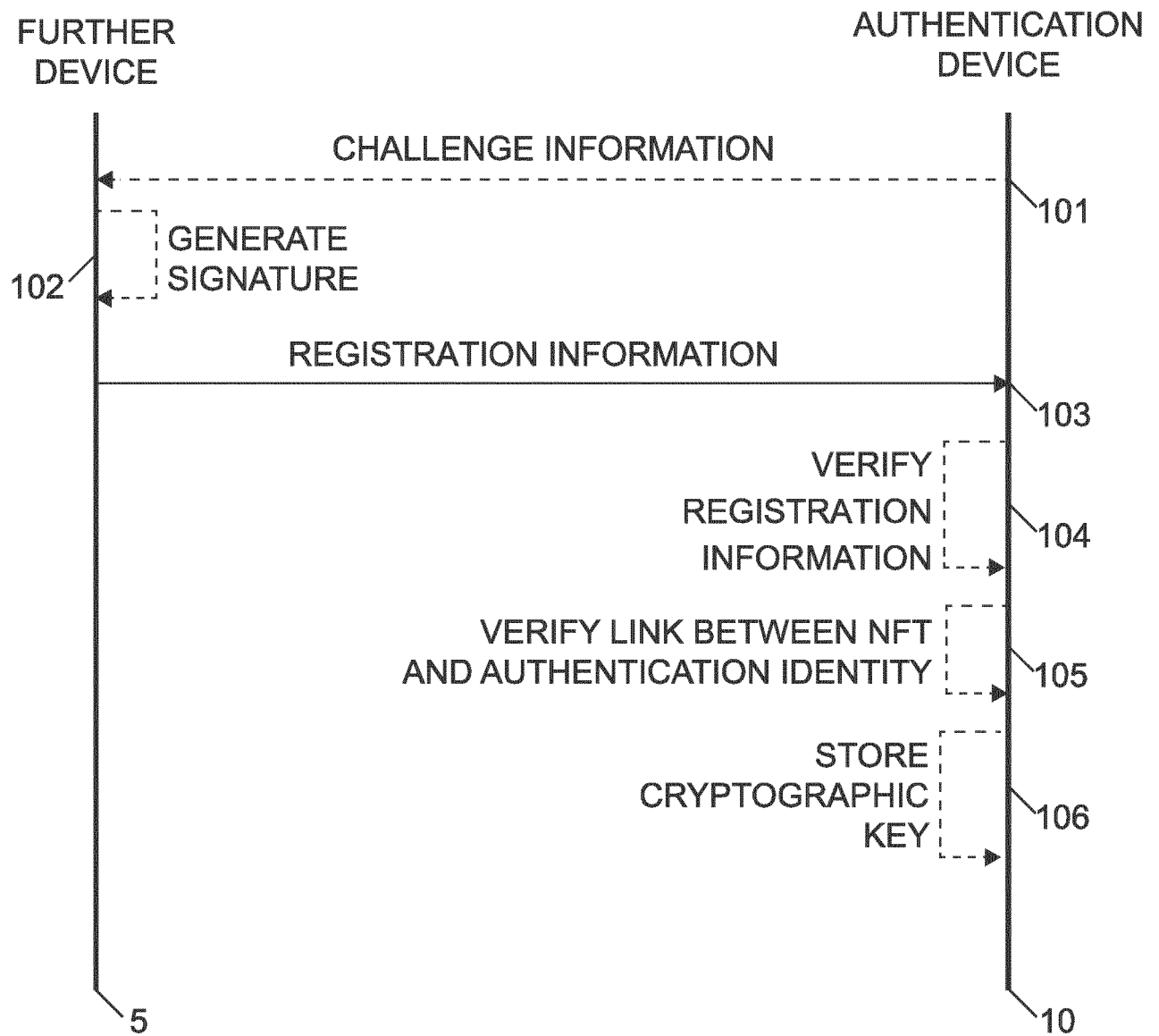


Fig. 1c

4 / 6

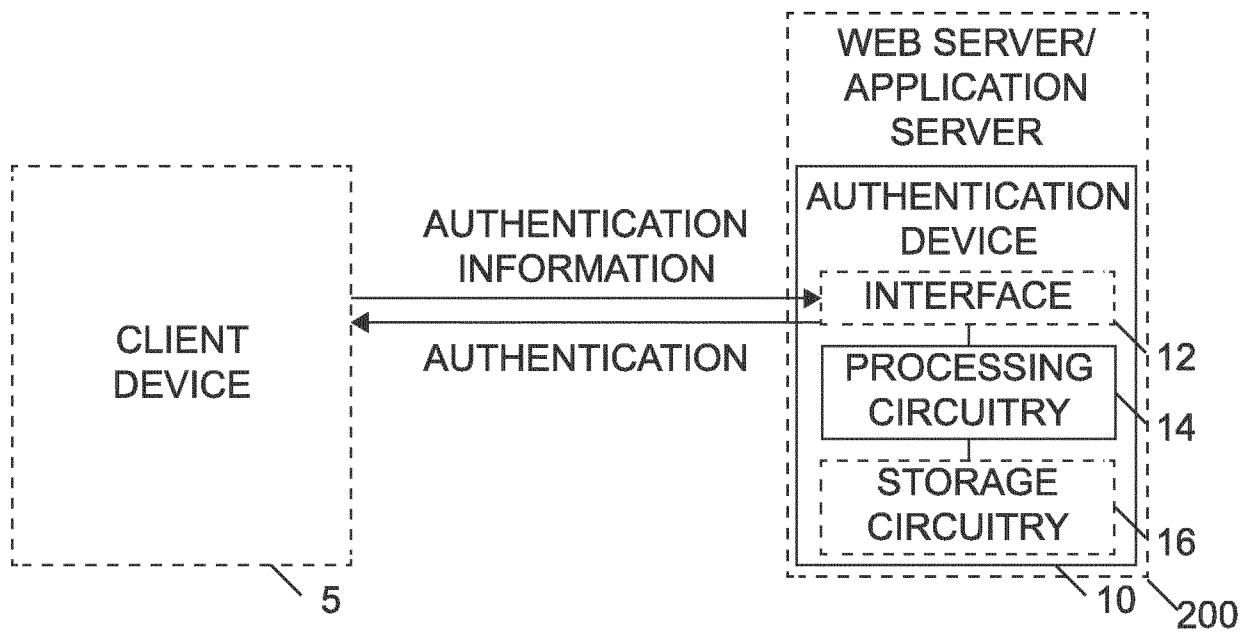


Fig. 2

5 / 6

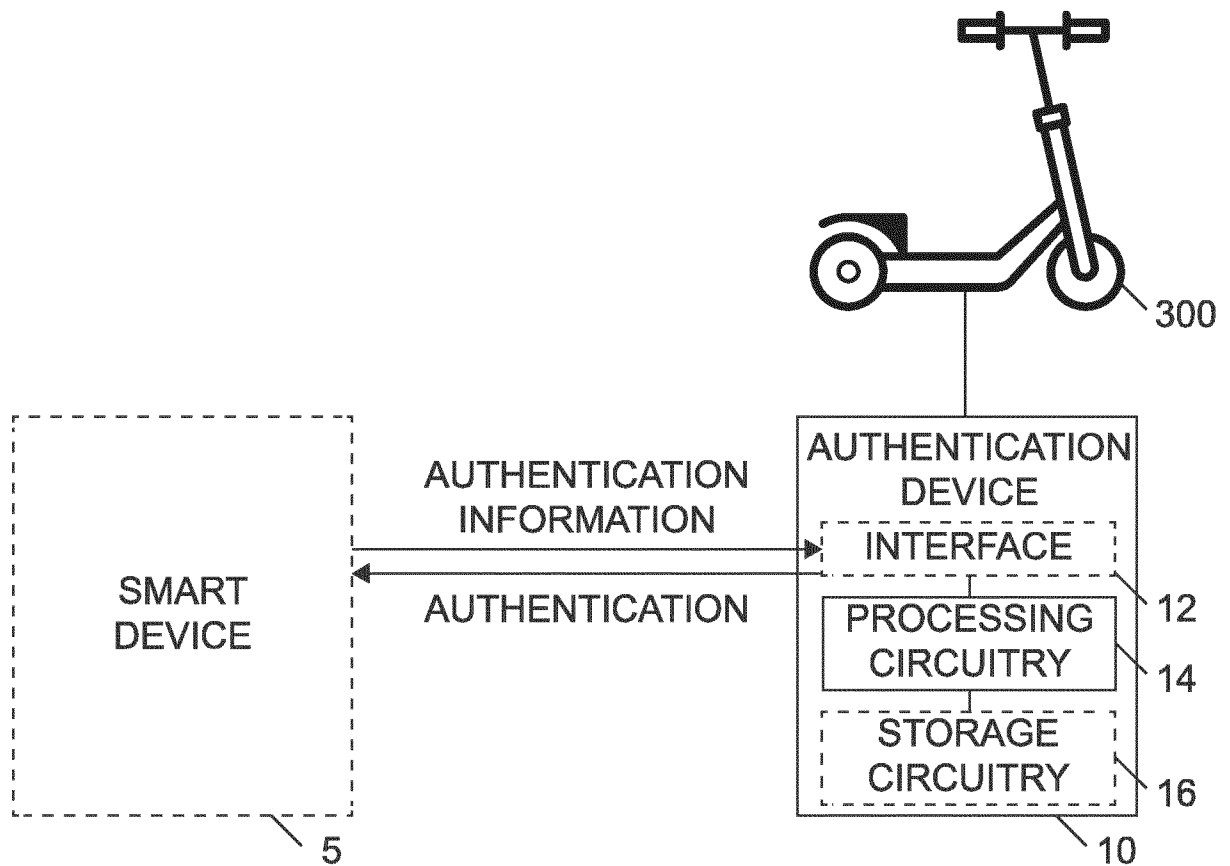


Fig. 3

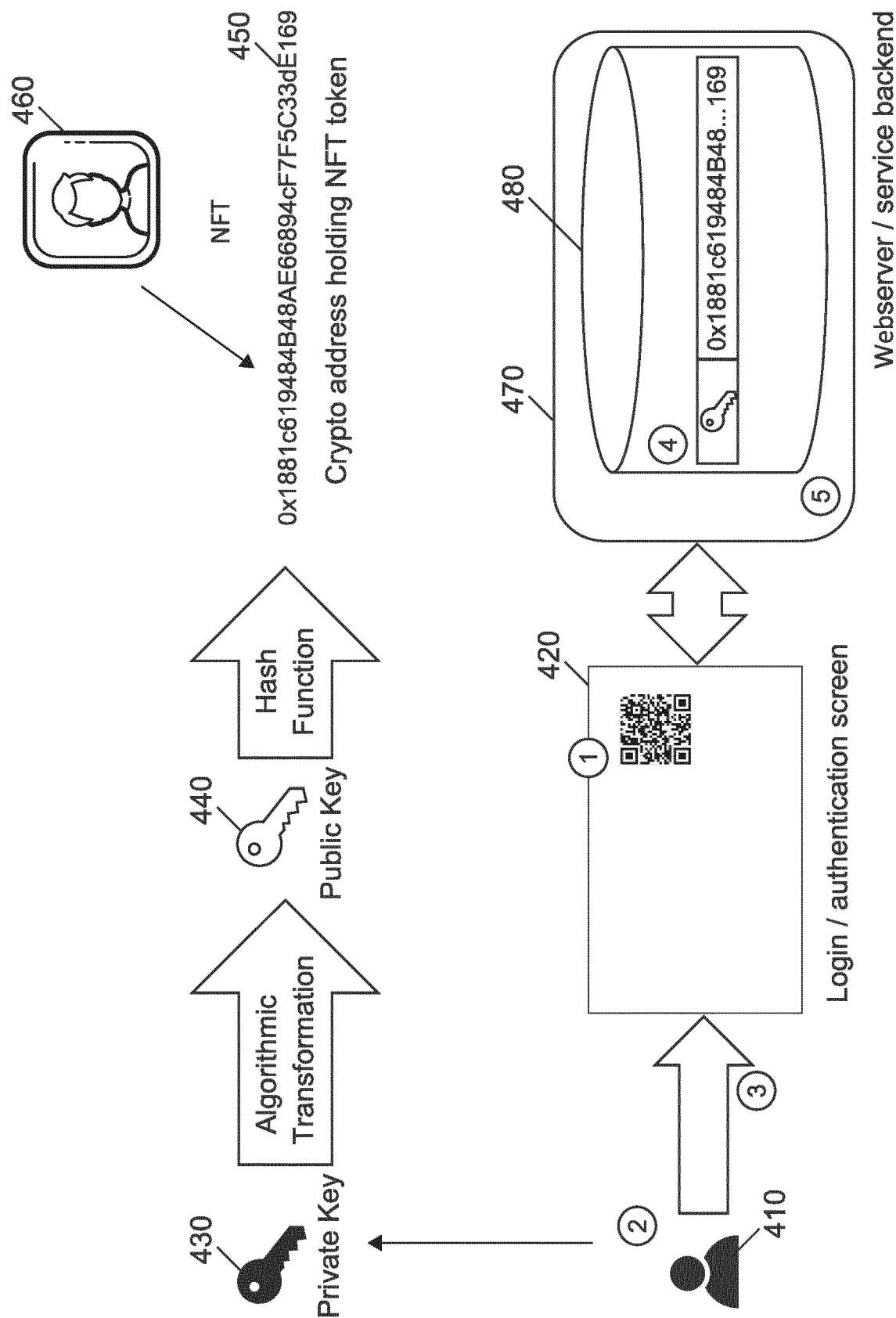


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2023/062045

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/40 H04L9/32 H04L9/00 G06F21/31 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/053081 A1 (PARK CHAN IK [KR] ET AL) 13 February 2020 (2020-02-13) paragraphs [0027], [0032], [0053], [0057] - [0061], [0068], [0090] - [0092]; figure 7 -----	1-14, 17-20
X	JP 6 978168 B1 (NISHIZAWA KATSUYA) 8 December 2021 (2021-12-08) paragraphs [0012] - [0013], [0016] - [0018], [0027] - [0029], [0039] - [0040], [0294] -----	1-20
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
12 July 2023		20/07/2023
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Veillas, Erik

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2023/062045

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020053081 A1	13-02-2020	KR 20200018967 A	21-02-2020
		US 2020053081 A1	13-02-2020

JP 6978168 B1	08-12-2021	JP 6978168 B1	08-12-2021
		JP 2022109467 A	28-07-2022
		WO 2022154051 A1	21-07-2022
