AUTHENTICATION METHOD AND SYSTEM TO VERIFY THE OWNERSHIP OF AN ITEM

Raffaele Bini
CTO
1TrueId srl
Chiari (BS), Italy
cto@1trueid.com

Fausto Chiappa
CEO
Sait srl
Chiari (BS), Italy
fausto.chiappa@saitweb.it

I. ABSTRACT

Authentication method to verify the authenticity of items, including associating to each item an electronic identification device having a unique identification code, selecting at least one piece of item information suitable to describe the item, associating to each identification code at least one respective and unique encryption key, encrypting the identification code and the item information, storing the encrypted content in the memory of the electronic identification device (for example a RFID tag), obtaining the identification code and the encrypted content from the electronic identification device, decrypting the encrypted identification code using the encryption key corresponding to the obtained identification code, in case of correspondence between the decrypted identification code and the obtained identification code, decrypting the encrypted item information using the encryption key. Data are stored in a Non Fungible Token on a suitable Blockchain that represents a digital twin of the electronic identification device, including a method to verify the ownership of the NFT with corresponding RFID tag.

II. DESCRIPTION

A. Blockchain Tokens

The authentication methods described later include the recording of the encrypted UID and encrypted information in a Blockchain.

Each owner who interacts with the Blockchain has a digital identity, identified with a wallet that contains a public key (the wallet address) and the private keys needed to sign transactions in the blockchain. For example the piece of item information that includes the ownership of the item is the public key of the identifying wallet of the manufacturer or supplier of the item, indicated at 1 in the accompanying figures.

The wallet contains private keys needed to control the coins or/and the NFTs (Non Fungible Token) or any other digital object stored in blockchain associated with that address. These NFTs will be used to represent physical item in the Blockchain. Each NFT must be created by an entity that is authorized to do so.

The creation of the new Blockchain object is only allowed to certain subjects, called "makers", identified with the manufacturers of the items themselves. Each manufacturer has a digital identity in Blockchain with the necessary permissions to be able to create new objects.

The "makers" can then transfer the "ownership" of the created object to other entities, which can be identified as distribution centers, retailers or directly end customers. Each transfer of ownership generates a new transaction in the Blockchain and with each transfer the change of ownership of the object is recorded, that is, the object is transferred from the wallet of the old owner to the wallet of the new one.

The real distribution chain, which involves the passages from maker to distributor, from distributor to retailer, from retailer to final customer, are modeled with the mechanism of ownership transfer.

With reference to Fig. 1a and 2a, the steps for creating a new object are the following:

When the generation of an encrypted content is requested for the creation of a new object, the authentication server that takes care of encrypting the data performs the following operations:

- encrypts the UID and item information to yield encrypted content (step 204);
- contacts the Blockchain service for creating an object in a Blockchain, the object including the encrypted content (step 204a)
- returns the encrypted data to the device that takes care of saving the encrypted data on the memory of the electronic identification device (tag RFID, for example). The tag can be written with the encrypted data (step 206).

The steps for verifying an object are described below.

When the verification of the encrypted content of a tag is requested (tag reading), the authentication server:

- decrypt the encrypted content, to obtain decrypted UID (step 210; 304);

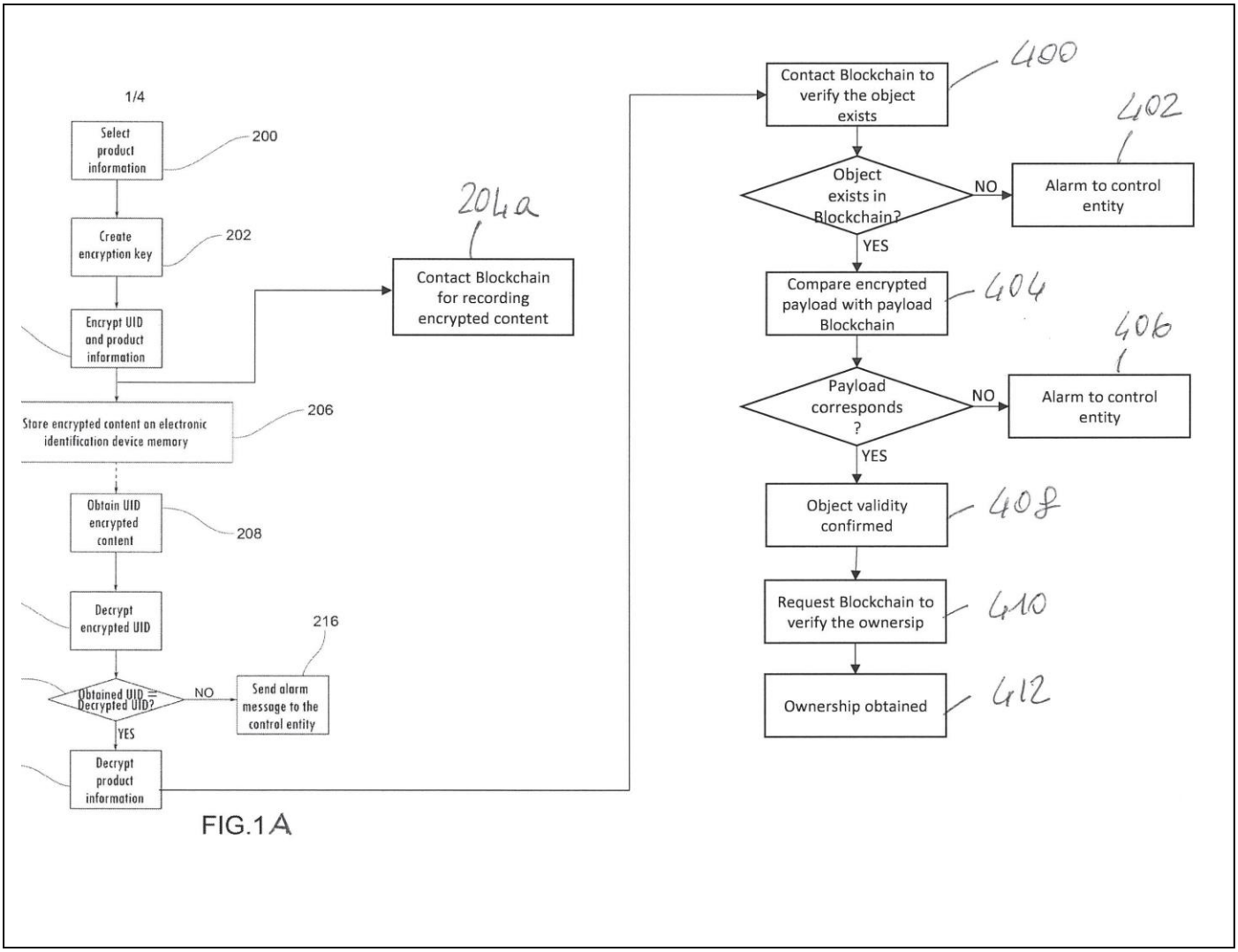

FIG.1A

- compares the UID of the tag with the encrypted UID (step 212; 306);
- if there is no correspondence, sends an alarm to a control entity or to the subject that asked for the verification of the object (step 216; 312);
- if there is a correspondence, then decrypts the item information (step 214; 308).

The authentication server or the verification device contacts the Blockchain service for verifying the existence of the object in the Blockchain (step 400).

If the Blockchain service determines that the object does not exist in the Blockchain, an alarm is sent to a control entity or to the subject that asked for the verification of the object (step 402).

If the Blockchain service determines that the object exists, the Blockchain service checks that the encrypted content (i.e., the payload) of the object to be verified matches the encrypted content of the object in the blockchain (step 404).

If there is no correspondence, an alarm is sent to a control entity or to the subject that asked for the verification of the object (step 406).

If there is a match, the Blockchain service confirms the validity of the object to the authentication server or to the verification device (step 408).

The authentication server or the verification device requests the Blockchain service to verify the ownership of the object (step 410).

The authentication server or the verification device may use theinformation about the ownership provided by the Blockchain service to update the item information (step 412). For example, the updated item information is encrypted by the authentication server and the encrypted updated item information is sent to the verification device for being written in the memory of the electronic identification device.

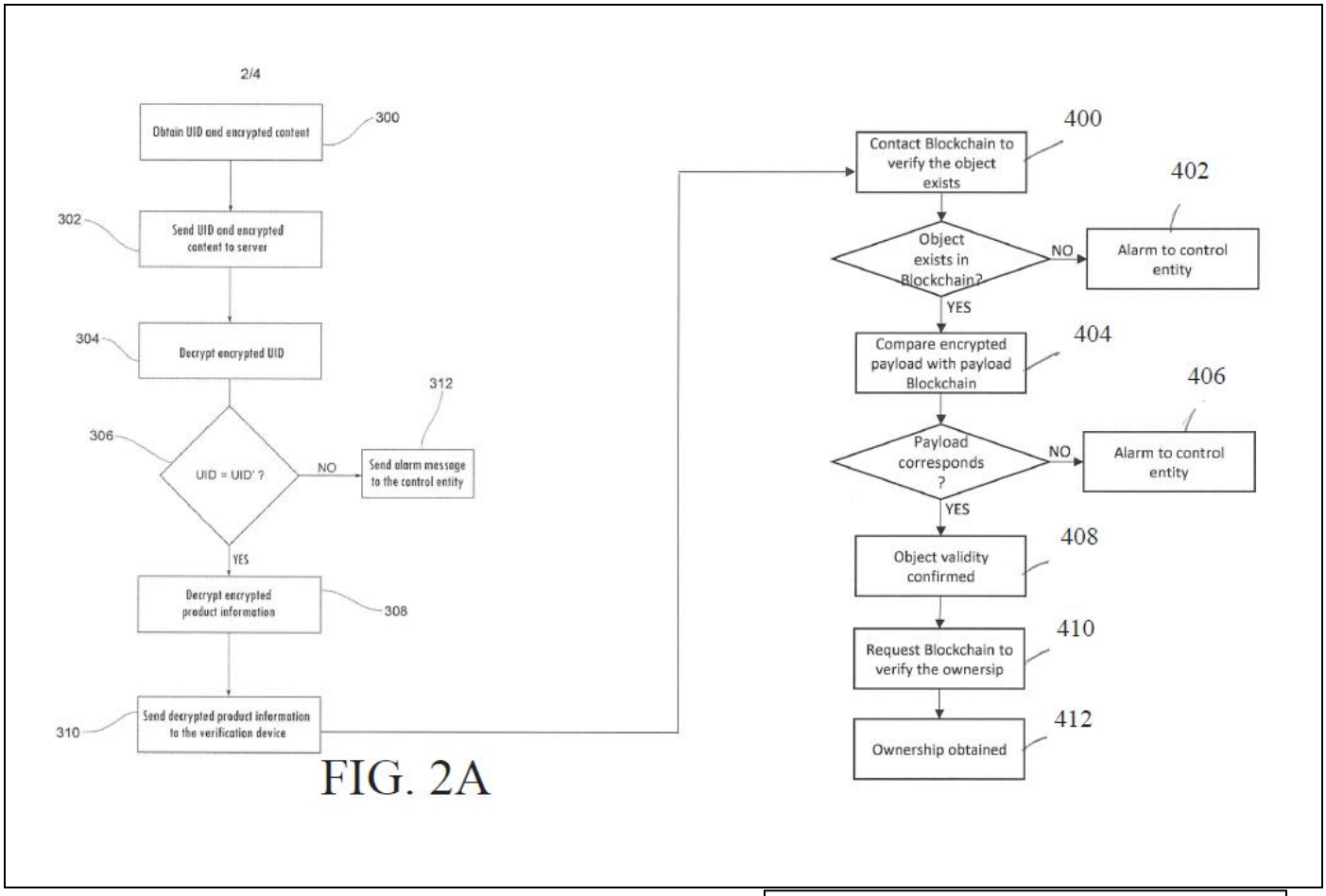

FIG. 2A

B. Ownership Method

Fig. 3 is a block diagram of the method for requesting the Blockchain service to record a change of ownership of an object.

The request can be made by an entity (the "new owner") that receives the object from another entity (the "old owner), for example a distribution center receiving the object from the maker, or a retailer receiving the object from a distribution center, or, preferably, can be made by an entity that sells or donates the object to another entity (for example a transfer of ownership between a retailer and a customer or between end-users or customers). In the latter case, the "old owner" must know the digital identity of the "new owner" in the Blockchain.

In step 500, a verification device sends the Blockchain service a request to verify the ownership of an object. For example, the verification device transmits to the Blockchain service the encrypted content read from the electronic identification device (tag) of the object and/or the digital identity associated to the verification device.

The Blockchain service returns the verification device the information about the ownership (step 502).

If the owner corresponds to the new owner of the object, the process ends (step 504).

If the

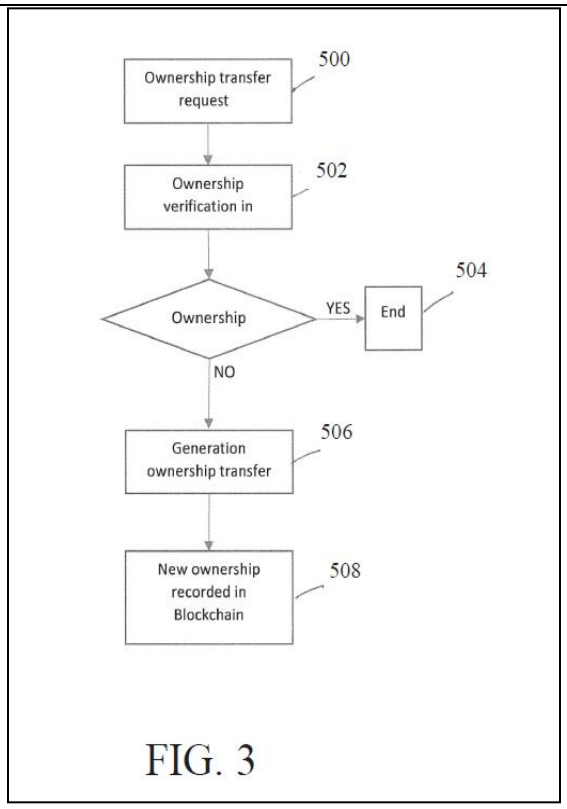

FIG. 3

owner does not correspond to the new owner, the verification sevice requests the Blockchain service to transfer the ownership of the object (step 506) and to record the information about the new ownership (step 508).

As explained above, the information about the new ownership may be used by the authentication server or directly by the verification device to update the item information, encrypt the updated item information and 15 store the encrypted updated item information in the memory of the electronic identification device.

C. Authentication Method

Fig.4 is an authentication system to verify the authenticity of items which implements the methods described above.

The authentication system comprises an electronic identification device 12 associable to each item 10. As mentioned above, each electronic identification device 12 is uniquely identified by an identification code 122 and is provided with a memory 14 in which an encrypted content 122'-18' is stored.

This encrypted content 122'-18' comprises, in encrypted form, the identification code 122 and at least one piece of item information suitable to describe the item.

Furthermore, each electronic identification device 12 is also suitable for being queried by a verification device 16 to transmit to such verification device the identification code 122 and the encrypted contents 122'- 18'.

The system furthermore comprises encryption means that use a set of encryption keys 20, each uniquely associated to a respective identification code 122, to encrypt the identification code 122 and the item information 18.

In one embodiment, said encryption means are also suitable to write to the memory 14 of each electronic identification device 12 encrypted content comprising the encrypted identification code 122' and the encrypted item information 18'.

In one embodiment, each identification code 122 is associated with a pair of encryption keys 20 suitable to implement an asymmetric encryption algorithm.

The authentication system also comprises at least one verification device 16 suitable for querying the electronic identification device 12 to obtain from it the identification code 122 and the encrypted content 122'-18'.

For example, the verification device 16 is composed of a generic mobile device owned by a user, such as a smartphone or a tablet, equipped with software suitable for querying the electronic identification device 12 and to implement the authentication method described above.

In one variant of embodiment, the verification device 16 may be a device specifically dedicated to perform the function of controlling the identity of the electronic identification device, e.g. used by a control entity or by a store that sells items equipped with an electronic identification device, etc.

The authentication system further comprises decrypting means suitable for decrypting the encrypted identification code 122' using the encryption key 20 corresponding to the obtained identification code 122, verifying the correspondence between the decrypted identification code and the identification code obtained from the verification device, and decrypting the encrypted item information 18' using the encryption key 20.

In particular, the decrypting means comprise software able to extract from the memory 14 of the electronic identification device 12 the content portion that should correspond to the encrypted identification code 122' and, in case of correspondence between the obtained authentication code and such decrypted content portion, obtain and decrypt also the remaining content of the encrypted memory.

In one embodiment, the authentication system comprises an authentication server 30 provided with encryption means and decryption means.

In this case, the verification device 16 is suitable to send to the authentication server the identification code 122 and the encrypted content 122'-18'. The decryption means are also suitable for returning the decrypted item information 18 to the verification device 16 (figure 3).

In one variant, the authentication system comprises an authentication server 30 provided with encryption means (20a).

The decryption means (20b) are installed on or accessible from the verification device 16.

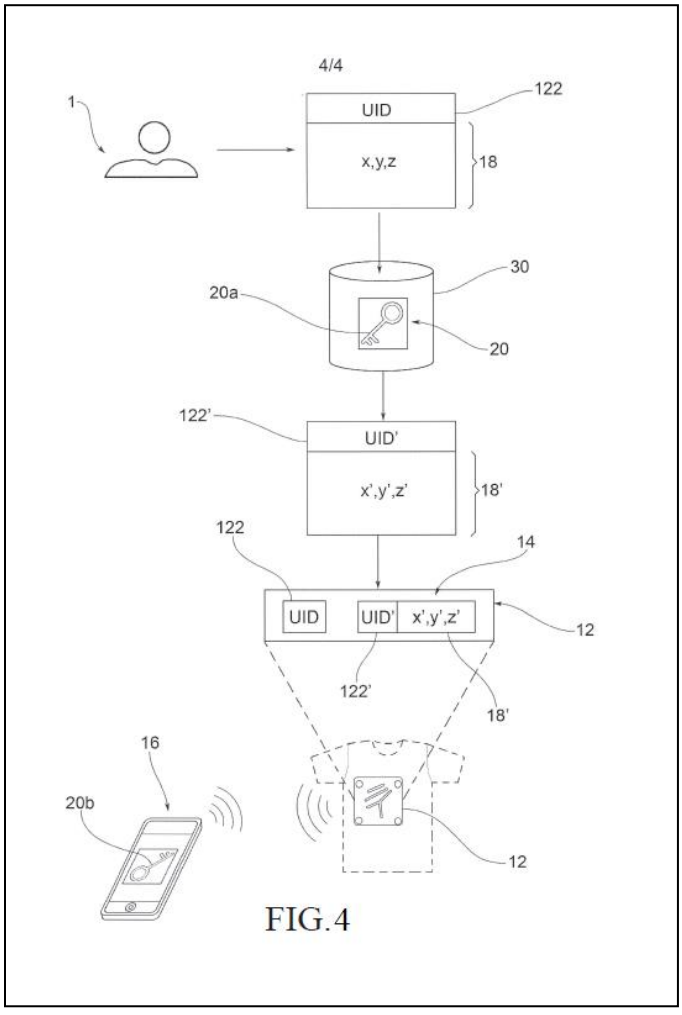

FIG.4

The verification device 16 is also configured to write an encrypted piece of user information to the memory 14 of the electronic identification device 12. The user information may be encrypted directly by the verification device 16, provided with encryption means, or by means of the authentication server 30, which receives the user information from the verification device, encrypts it, and returns it to the verification device to be written to the memory of the electronic identification device.