Clasp and piece of jewelry, methods, readout device, cloud storage system, personal identification device, and wearable device

The application relates to a clasp and a piece of jewelry comprising such a clasp.

A piece of jewelry may, for example, be a necklace or a bracelet. Such pieces of jewelry are typically embodied such that they can be secured to a wearer and can also be released. For that purpose, pieces of jewelry may have a clasp.

It is an object to provide for a clasp that is alternative or better compared with known solutions. It is also an object to provide for a piece of jewelry comprising such a clasp.

The application relates to a clasp, comprising a first element and a second element. The first element has a protrusion, and the second element has a clearance for receiving the protrusion of the first element such that the first element is rotatable with respect to the second element. The first element has an arm, and the second element has a gap, wherein the arm engages the gap when the first element is rotated with respect to the second element into a closed state. The first element is removable from the second element when the arm does not engage the gap.

This allows for a simple design of a clasp. The two elements may be separated from each other in an open state. They may be securely connected in a closed state. The closed state may be reached easily by engaging the protrusion with the clearance and by rotating the arm such that it engages the gap. By doing the opposite, e.g., rotating in the opposite direction and removing the first element from the second element, the clasp may be put in a state in which the two elements are separate from each other. For example, a wearer may put a necklace comprising such a clasp around her neck when the two elements are separate from each other. Then, the clasp may be brought into the closed state as described, and the necklace is secured to the wearer.

When the arm engages the gap, this may also be denoted that the arm goes through and/or is partially inside the gap.

The arm may especially protrude from a central part or main part of the first element from which also the protrusion protrudes. Such a main part may provide for a form fit with the second element, providing a secure connection of the two elements.

According to a possible implementation, the protrusion has a circular cross section. It may also have a cylindrical shape. This allows for easy rotation of the first element relative to the second element.

According to a possible implementation, the clearance has a circular cross section. It may also have a cylindrical shape. This also allows for easy rotation of the first element relative to the second element, especially in combination with a circular or cylindrical protrusion. If both the protrusion and the clearance have circular cross sections, this allows for a definition of the rotatability of the two elements relative to each other that is independent of a current rotation angle.

If the clearance mates the protrusion, this allows for an easy fit of the elements to each other. Mating may especially mean that there is no, or at least almost no, slackness between the protrusion and the clearance when the protrusion is received in the clearance.

Especially, the gap can be defined between a cantilever and a main part of the second element. The main part may especially comprise the clearance. The cantilever may especially protrude from a wall that is part of the second element. The cantilever may be at least slightly deformable, which can be used in order to provide for a retaining functionality as described below. The main part of the second element may provide for a base of the second element and even of the entire clasp. It may provide for stability and define, for example, a surface on which the clasp may lay on an underground. The clearance may be provided in the main part so that forces entering from the first part are, at least partially, absorbed by the robust main part.

According to a possible implementation, the gap has, at an end at which the arm enters the gap from an open state, a retaining element, the retaining element releasably retaining the arm in the gap. Thus, an inadvertent release can be prevented, especially by a form fit between the gap and the arm and by additional form fits that may be provided between the first element and the second element, especially a form fit that is achieved by receiving the protrusion in the clearance.

If the retaining element is embodied as a sphere partially closing an entry of the gap, this allows for a smooth passing of the arm and for an easy manufacturing of the retaining element by forming processes, along with securely retaining the arm in the gap.

The retaining element may especially be positioned at a free end of the cantilever. Thus, a certain resiliency of the cantilever may be used for releasably securing the arm in the gap. The free end may especially be an end opposite to an end at which the cantilever is secured to the rest of the second element, for example to a wall.

Especially, the first element may be not removable from the second element when the arm engages the gap. Thus, an inadvertent removing can be prevented. A form closure between the arm and the gap can be used.

The fist element can have a first loop for securing another element, for example a chain or another part of a piece of jewelry. The first loop may comprise a first hole, in which another element can be secured by form fit.

The second element can have a second loop for securing another element, for example a chain or another part of a piece of jewelry. The second loop may comprise a second hole, in which another element can be secured by form fit.

A form fit for securing another element like a chain to a loop may simply extend a means for securing chain elements to securing the chain to the clasp.

In other words, a loop allows for easy attachment of a chain.

According to a possible implementation, the first element and/or the second element comprise are magnetic element so as to attract each other by magnetic force. For example, one element or both of the first and second elements may comprise a magnetic element, which may especially be a permanent magnet. For example, a neodymium magnet can be used as magnetic element. Magnetic elements help securing the two elements to each other, especially when coming from an open state. The magnetization may especially be such that the two elements are automatically brought into a correct orientation relative to each other.

In a specifically advantageous implementation, both the first element and the second element each have a respective magnetic element. This can provide for helping a user to bring the both elements in a correct position for securing them together. However, it is also possible that only one of the first and second element has a magnetic element that is a permanent magnet. A magnetic field of such a magnetic element may interact with the other element that may be fully or partially made of a magnetically active material, for example a diamagnetic material. This may lead to a magnetically attracting effect between the two elements. However, it may be harder or impossible to implement an attracting force between the two elements that automatically helps to bring the two elements in a correct orientation.

Especially, the first element may comprise a first magnetic element forming the protrusion. Especially, a part of the first magnetic element may form the protrusion. Another part may be secured in a main part of the first element. The first magnetic element may especially have a cylindrical or disc shape.

Especially, the second element may comprise a second magnetic element being positioned in the clearance. Especially, the second magnetic element may have a cylindrical or disc shape that mates the clearance. Thus, the clearance can be partially filled with the magnetic element, while the rest of the clearance may be left to receive the protrusion.

These implementations allow for an advantageous reception of the magnetic elements such that they attract each other in a way that the first element and the second element are automatically brought into the correct orientation.

The first element and/or the second element may be fully or partly made of gold, silver, metal, or metal alloy. These materials may provide for a good matching to common materials used in jewelry fabrication. Especially, all but a respective magnetic element can be made of such a material. However, also other materials may be used.

According to a possible implementation, the second element has a wall encompassing a segment of a circle and laterally securing the first element when the protrusion is received in the clearance. This helps stabilizing the elements. It can also prevent the first element from inadvertently being released from a position in which the protrusion is received in the clearance.

The clasp may comprise an identification tag in the first element, the second element, or between the first element and the second element. Such an identification tag may, for example, be embodied as an RFID (radio frequency identification) tag or as a nanotech structure. It can especially have a unique ID for identifying the clasp. This can ensure traceability and identifiability of a specific clasp. It may, for example, be used for inventory control and as a personal ID. It is also possible that more than one such identification tags are used. For example, such an RFID tag can be used as described elsewhere herein. Reference is made to the plurality of different implementations.

The application relates further to a piece of jewelry, especially a necklace or bracelet, comprising a clasp as described herein. With regard to the clasp, all embodiments disclosed herein can be applied. Disclosed advantages of the clasp also apply for the piece of jewelry.

The piece of jewelry may comprise at least one chain being attached to the first element and/or to the second element of the clasp. Such a chain may, for example, be used to secure gems and/or may be used as a design element itself. Especially, the chain may be secured to loops with their holes as described herein.

The clasp, the first element, and/or the second element can be made partly or entirely of several materials, among them gold and silver, as well as from alloys with these materials, that can also comprise other materials such as copper. It is also possible to make these from a polymer, such as plastic, or from wax. A wax model can then be easily used in a cast or molding method for producing multitudes of the clasp, the first element, and/or the second element from metals or precious metals.

The application relates further to a method for retrieving user-related information, to a method for performing a payment process, to a method for providing user-related information, to a readout device, to a cloud storage system, to a personal identification device, and to a wearable device.

In many situations, it can be preferable to have user-related data readily available. For example, payment information is typically needed after dining in a restaurant. Another example is a conference, where conference participants can benefit from knowing who has similar interests.

It is an object to provide for methods in the context of user-related data, user interaction or inventory control that are alternative or better compared with known solutions. It is also an object to provide for a readout device, a cloud storage system, an identification device, and to provide for a wearable device.

The application relates to a method for retrieving user-related data from a cloud storage system, the method comprising the following steps:

- reading out an identification number from an RFID tag,
- providing a variable, a content of the variable indicating a type of user-related data, preferably using an interface device,
- sending a request comprising the identification number and the content of the variable to the cloud storage system, and
- receiving user-related data from the cloud storage system, the user-related data preferably being based on the identification number and the content of the variable.

With such a method, a wearable device can be used in order to retrieve data based on an identification number stored in an RFID tag. The wearable device may, for example, be a piece of jewelry, a clasp, a watch, or another device that can easily be held by, or secured to, a human being.

The RFID tag may especially be secured in a wearable device, for example in a clasp, another piece of jewelry, a watch, or a piece of clothing.

The variable may be implemented as an electronic variable. It may comprise several bits that define its content. The content may be indicative for a type of user-related data. Each specific bitstring may be indicative for a specific type.

The type of user-related data typically defines which user-related data is requested. Typical examples are given below. Different types may be made available to serve different situations.

The request may, for example, be sent using the Internet and may especially be sent using a wireless and/or wire-bound connection. The cloud storage system can be a database or similar system located anywhere on the internet, especially being configured to be accessible by a device performing the method.

According to a possible implementation, the content of the variable and/or the type may be provided by a device performing the method. Especially, the type may be set by such a device, for example by preprogramming or by a functionality of the device identifying a location or another parameter and setting the type based thereon. Providing the type, or a corresponding content of the variable, may define which user-related content is to be retrieved.

According to a possible implementation, the content of the variable and/or the type may be provided by user input. Especially, the device performing the method may be configured to ask for the user input and to retrieve the user input. A display or a touch-screen may be used for that purpose. However, also other means of input may be used.

When the type is out of a first group of types, only the identification number and the type may be sent to the cloud storage system. This allows defining a group of types, wherein types being part of this group do not need additional security measures. For example, simple user data or information about the wearable device may be part of this first group.

When the type is out of a second group of types, at least one security information may be obtained and may be sent in addition to the identification number and the type to the cloud storage system. This allows defining a group of types, wherein types being part of this group need additional security measures. For example, payment information or medical information may be part of the second group.

It may be implemented that obtaining security information comprises taking a fingerprint, and the security information may comprise information regarding the fingerprint. Thus, a fingerprint may be used as a readily accessible security feature. A fingerprint reader may be used for that purpose. A reference fingerprint may be stored in the cloud storage system for identifying if the user of the RFID tag is authorized.

Additionally or alternatively, obtaining security information may comprise taking a speech record, and the security information may comprise information regarding the speech record. Thus, a microphone or another device may be used in order to record a speech sample of a user. The speech may be used by the cloud storage system to compare with a stored voice sample and to identify if the user of the RFID tag is authorized.

Additionally or alternatively, obtaining security information may comprise taking a picture of a face, and the security information may comprise information regarding the picture of a face. Thus, face recognition may be used to identify an authorized user. For example, a movement of an eyebrow or another face identification means can be used.

Additionally or alternatively, obtaining security information may comprise inputting a code, and the security information may comprise information regarding the code. For

example, the code may be a PIN number or an alphanumerical code. A reference code may be stored in the cloud storage system and may be used in order to identify an authorized user.

A possible type may be ownership information. For example, a user's name or address may be part of the ownership information. The ownership information may be part of the first group, so that no specific security measures are required.

A possible type may be medical information. For example, medications or blood group may be part of the medical information. The medical information may be part of the second group, so that additional security measures are required.

A possible type may be meet and greet information. For example, a name, an affiliation, or a purpose for visiting a conference or an exhibition may be part of the meet and greet information. The meet and greet information may be part of the first group, so that no specific security measures are required.

A possible type may be personal preference information. For example, a meat or wine preference, food allergies, preferred colors of clothes, or preferred materials can be part of the personal preference information. Thus, a waiter may be readily informed about what food to offer. Likewise, a shop owner may be readily informed about which clothes to offer. The personal preference information may be part of the first group, so that no specific security measures are required.

A possible type may be payment information. For example, banking or credit card details may be part of the payment information. Especially, such payment information may be used for payment in a restaurant or a shop. The payment information may be part of the second group, so that specific security measures are required.

The possible types may be combined in a specific implementation.

The received user-related data may be presented on a screen of a device performing the method. This may allow the data to be readily accessed by the user of the RFID device or another person like a waiter or shop owner. For example, the device may

be configured to read out the identification number, to send the request to the cloud storage system, to receive the user related data, and/or to present the data on a display or screen.

The method may be performed in a mobile electronic device, a tablet, or a stationary electronic device. A mobile electronic device may, for example, be a mobile phone or a specific device used for payment or other purposes. A tablet may especially be a larger portable device with a large screen. A stationary electronic device may be positioned at a shop or restaurant entrance to allow user identification and retrieving of preferences or other user-related data.

The application also relates to a device, for example a mobile electronic device, a tablet, a stationary electronic device, or a mobile phone for performing a method as disclosed herein. The application also relates to a non-transitory computer-readable medium comprising program code that cause a processor to perform a method as disclosed herein. With regard to the method, all variations as disclosed herein can be applied. The device may be a readout device as defined elsewhere herein.

Especially, the RFID tag may be a passive RFID tag. Thus, no energy consumption is needed by the RFID tag. The passive RFID tag may be read out by radio waves emitted by a readout device. It does not need a separate power source.

The application further relates to a method for performing a payment process, the method comprising the following steps:

- reading out an identification number from an RFID tag secured in a wearable device,
- setting a content of a variable for defining a type of user-related data to be payment data,
- requesting security information,
- obtaining security information,
- sending a request comprising the identification number, the content of the variable, and the security information to a cloud storage system,
- receiving user-related data being payment data from the cloud storage system, and

- performing the payment process using the payment data.

This method allows for a specific payment process that is very easy to perform, as payment data can be retrieved from the cloud storage system and can be readily made available based on the automatic read out RFID tag. No credit card, coins or the like is needed. The security information ensures that only an authorized user, i.e., the owner of a wearable comprising the RFID tag, may initiate the payment process.

With regard to the method for performing a payment process, reference is made to the statements given above with regard to the method for retrieving user-related data, which can be readily applied.

Especially, the security information may be a fingerprint, a voice record, a picture of a face, or a code. Reference is made to the statements given above.

The payment process may be a process of paying a bill, for example in a shop or a restaurant. It may also be a process of retrieving money at an ATM or similar device.

According to a preferred implementation, the method may further comprise a step of selecting which kind of security information should be requested. This gives the user a choice and gives him the possibility to select the security information that is most suitable in the specific case. For example, a face picture or a code may be chosen in a noisy environment, while speech recognition may be selected by a person whose face is covered by a mask.

The selecting may be performed by user input. For example, respective buttons may be pressed on a touch screen display.

The selecting may alternatively or additionally be performed automatically based on an amount to be paid, a location, a venue, and/or based on other information. For example, a device operated in a shop, or a restaurant may require a specific security information, for example a fingerprint, if the amount to be paid is larger than a threshold.

Especially, the payment data may be based on the identification number. Specifically, the cloud storage system may generate the payment data based on the identification number.

The application further relates to a method for providing user-related information to a person, the method comprising the following steps:

- reading out an identification number from an RFID tag secured in a wearable device,
- setting a content of a variable for defining a type of user-related data to be meet and great information or personal information,
- sending a request comprising the identification number and the content of the variable to a cloud storage system,
- receiving user-related data from the cloud storage system, and
- presenting the user-related data on a display and/or sending the user related data to another electronic device.

This method can easily provide information to a person. The person may be the user or may be another person. For example, the person may be a waiter in a restaurant or may be a shop owner or shop employee who needs information about a customer entering the shop.

With regard to that method, reference is made to the details and variants described above, which may be readily applied.

The application further relates to a personal identification device, comprising

- a tag holder for mechanical connection with a wearable device, and
- an RFID tag being mechanically connected with the tag holder,
- wherein the RFID tag has stored, or is configured to store, an identification number.

Such a personal identification device may be used in order to provide an RFID tag, especially in a wearable device. The RFID tag may be used in connection with the method as described above. It may uniquely identify its wearer.

According to an implementation, the tag holder may be fully or partially made of a precious metal. This allows high resistance against corrosion. However, also other methods may be used.

The RFID tag may have a round, rectangular, or square shape. That may fit in respective openings or recesses of wearables. The shape may be seen in a cross section. However, also other shapes may be used.

The RFID tag may have a diameter of at least 1 mm and/or of at most 4 mm. Such sizes fit in typical wearables and provide the required functionality.

If the RFID tag is round or at least substantially round, the RFID tag may preferably have a diameter of 1.5 mm or 3 mm. It may also be smaller or larger.

If the tag holder forms an antenna or an antenna amplifier for the RFID tag, the signal of the RFID tag may be amplified and may thus be easier read out. The tag holder may thus provide an additional functionality.

The application further relates to a wearable device, comprising

- a fastening structure for fastening the wearable device to a human body, and
- a personal identification device as described herein.

With regard to the personal identification device, all embodiments and variants as disclosed herein can be applied.

The wearable device may have a specific functionality, like a watch, and furthermore may be used to identify the user. Especially, the methods described herein may be used for that purpose.

The wearable device may be a mechanical watch. The RFID tag may, for example, be embodied in a clockwork of the watch. This makes an unauthorized exchange very complicated and secures integrity of the RFID tag with the watch. The RFID tag may also be secured to other mechanical parts, for example a watch strap clip, clasp, or spectacle frame.

The wearable device may be a piece of jewelry. For example, it may be a necklace, an earring, a bracelet brooch, or a clasp. It may hold a gemstone, for example a diamond. Especially, the RFID tag may be positioned under a gemstone setting, which protects the RFID tag against unauthorized exchange.

The wearable device may be a clasp. A clasp may be used to releasably secure two ends of a chain or other long flexible element to each other. A possible implementation is given elsewhere herein. All variations can be applied.

The tag holder may be soldered or lasered in the wearable device. This provides for a secure connection between the RFID tag and the rest of the wearable device.

The invention relates further to a readout device, comprising an RFID reader being configured to read out an identification number from an RFID tag, and an interface device being configured for

- providing a variable, the content of the variable indicating a type of user-related data using an interface device,
- sending a request comprising the identification number and the content of the variable to a cloud storage system, and
- receiving user-related data from the cloud storage system, the user-related data being preferably based on the identification number and the content of the variable.

The readout device can especially be configured and/or used to perform a method as described herein.

The readout device can typically send an interrogating signal to the RFID tag via an antenna, and the tag typically responds with its unique information. Especially, the readout device can be configured to read out a passive RFID tag.

Passive RFID tags primarily operate at three frequency ranges:
Low Frequency (LF): 125 -134 kHz
High Frequency (HF): 13.56 MHz

Ultra High Frequency (UHF): 856 MHz to 960 MHz

Near-field communication (NFC) devices operate at the same frequency (13.56 MHz) as HF RFID readers and tags. The standards and protocols of the NFC format is based on RFID standards outlined in ISO/IEC 14443, FeliCa, and ISO/IEC 18092. These standards deal with the use of RFID in proximity cards.

NFC devices can read passive NFC tags, and some NFC devices are able to read passive HF RFID tags that are compliant with ISO 15693. The data on these tags can contain commands for the device such as opening a specific mobile application.

The identification number stored in an RFID tag can be used to be linked with a specific person, who may be called the keyholder. The seller of a device comprising such an RFID tag, for example a clasp, may pair the identification number with a specific person.

Typical RFID tags can hold up to 16 digits.

The invention relates further to a readout device, comprising an RFID reader and an interface device, the readout device being configured to perform a method as disclosed herein. Especially, all methods and its variants disclosed with respect to reading out from an RFID tag and interacting with a cloud storage system or another device may be implemented.

The invention relates further to a cloud storage system, the cloud storage system being configured to

- receive a request comprising an identification number and a variable, the content of the variable indicating a type of user-related data, and
- send user-related data depending on the identification number and the conent of the variable.

Such a cloud storage system may especially interact with a readout device as disclosed herein. The user-related data may be sent to the readout device or other device from which the request was received. The cloud storage system may

especially be used in a method as disclosed herein. Reference is made to the statements given elsewhere herein. All variations can be applied. Especially, it may be possible to access the cloud storage system using standard internet access.

The cloud storage system may further be configured to receive security information, to compare the security information with stored reference data, and to send user-related data only if the security information corresponds to the stored reference data. This can implement the security functionality disclosed elsewhere herein. Especially, the disclosed types of security features may be implemented.

The invention relates further to a method for inventory control of a personal identification device, the method comprising the following steps:

- writing an inventory control number in an RFID tag, and
- tracking the personal identification device using the inventory control number.

Thus, the inventory control number can be used in order to give a company the possibility to identify stored items and to keep track of the inventory. Especially, inventory control may be performed before sale.

The inventory control number may be read out from the RFID tag each time an inventory should be determined. This can be done by a readout device accessing information stored on the RFID tag.

The invention relates further to a method for forgery control and/or theft control of a wearable device, the method comprising the following steps:

- reading out an identification number from an RFID tag of the wearable device,
- comparing the identification number to a reference dataset, and
- indicating forgery if the identification number does not correspond to the reference dataset, or indicating theft it the reference dataset indicates that the identification number corresponds to a stolen device.

Especially, a cloud storage system may be used when performing such a method. A readout device may read out the identification number and send it to the cloud storage system for further processing.

The invention relates further to a method for providing an electronic invoice for a wearable device, the method comprising the following steps:

- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to an invoice system, and
- providing an electronic invoice by the invoice system based on the identification number.

Especially, a cloud storage system may be used as invoice system. A readout device may read out the identification number and send it to the cloud storage system for further processing.

The invention relates further to a method for providing an electronic warranty card for a wearable device, the method comprising the following steps:

- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to a warranty system, and
- providing an electronic warranty card by the warranty system based on the identification number.

Especially, a cloud storage system may be used as warranty system. A readout device may read out the identification number and send it to the cloud storage system for further processing.

The invention relates further to a method for providing an electronic product information for a wearable device, the method comprising the following steps:

- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to a product information system, and
- providing an electronic product information by the product information system based on the identification number.

Especially, a cloud storage system may be used as product information system. A readout device may read out the identification number and send it to the cloud storage system for further processing.

A 1st level of security (low security level) may be implemented to generate an in-house EPC (electronic product code). Typically, the final attachment of an RFID tag is fixed on the product permanently at this time. The manufacturer may input an EPC (electronic product code) to the RFID chip for its inventory control and/or information of a product, such as weight of gems and gold or memo of holder.

A 2nd level of security (low security level) may be implemented, especially at retail level. Outlets can keep the same EPC number or rewrite a new in-house number while keeping information of a product for their inventory control. In addition, they may add their branding to the product.

A 3rd level (mid security level) may be implemented, especially for a time once the product is sold. A digital invoice, digital warranty, and ownership data is added to a cloud storage system or an in-house system control. Reference is made to the statements given elsewhere herein.

A customer may especially have a freedom of use. Specifically, a customer can choose to further activate or deactivate the RFID chip or RFID tag from a system.

A 4th level (high security level) may be implemented, especially in order to maintain an RFID system to be in use for further conveniency. A customer can register with a central system, for example a cloud storage system, by verifying, e.g., with their IC or passport to make sure the system is communicating with the right person and can complete four ways of security verification.

For security verification, face recognisation (FR), voice recognisation (VR), biometric fingerprint (BF), and/or a PIN number (PN) can be used. Also, other means can be used.

Once a system, especially a cloud storage system, receives an update of information, the system can generate a new EPC number as a personal identity or a digital key for the customer to install information in different level of security such as:

1st: storage of information: precious product bought that has RFID implant, for ownership information, and/or information of the product if it is lost and/or found or stolen.

2nd: personal medical data: used for emergency in a medical situation. It can be implemented that only an authority can override and/or retrieve information with a reader for only level 2 information.

3rd: personal meet and greet information such as self-portrait, name of entity, information, company advertisement or people the keyholder wishes to get in touch and hobby. At a conference or a meeting, a portable reader can be made available at the entrance and/or at the registration desk for the keyholder to scan his RFID identity (especially from the RFID tag) and the reader or another system can show the keyholder's presence or attendance. A user can choose to stay anonymously after register or can be made known by the RFID scanner system to share via Bluetooth or message to send information to those in the event. This will help to safe time to meet the right person the keyholder wishes to meet and enables to have a good follow-up after meeting. Hobbies are a great topic to break the ice in human interaction. Last is to keep update of who the keyholder met if another pandemic takes place.

4th: shopping and dining experience (option to install): a user can first install information such as how he wishes to be greeted, favorite colors, styles, or items they are looking forward to buy, favorite drinks, food or any food allergy.
At the entrance of a shop there may be an RFID reader with two system elements. The 1st is a monitor or screen where the keyholder is scanned and sees if he can find anything of great interest before stepping into the shop. As 2nd, once stepped in, staff can automatically receive information of the guests on their tablet with information needed to serve the customer.

As for dining, service staff in their tablet would know what not to recommend due to food allergy of customer, and information of their return customer's past orders.

The described implementation may help knowing the way how he or she likes it to be cooked and type of wine he or she likes. Such personal service cannot be achieved without a personal RFID identity. The system can capture information during payment.

During any payment, the customers can be served with a tablet that has a specific system build in for higher security check. Further reference is made to the statements given elsewhere herein, which can readily be applied.

At a 1st step, customers can scan the RFID tag as a key to operate the system. Once scanned, there may be a need to do a mid-level security check, e.g., by face recognition. A screen can appear with a welcome note and an option to take a photo of the keyholder. Next, a touch screen may be operated to process payment.

At a 2nd step, the customer can verify an amount, i.e. if it is correct in a digital invoice, and use a touch screen to process payment,

At a 3rd step, an electronic wallet screen can appear to present types of payment such as credit card or any bank facility which the customer already has approved to use. For example, a customer would just need to touch a screen to select payment.

At a 4th step, the system can ask for a type of process to activate. Facial expression on face recognition can be used to process payment, if the action does not match the system will decline payment. If the user is not in a noisy environment, he can also select voice recognition, which may use spectrogram or audio coding, which does not require any language. Once it matches specific records in the system, for example in a cloud storage system, the payment will process.

A biometric fingerprint may be used to match the records in the system to approve payment.

If the user is in a low or slow signal area the already mentioned three security features may be slowed down or may be unable to activate. Then, a PIN number may be the last option, and should typically be kept for low value transaction only.

Once approved, the user can choose to keep records of invoices in the system, e.g., for a maximum of 6 months, or may keep a printed invoice if needed.

Especially for a payment process, the 2nd level of security check, which may be the facial expression and voice recognition for the payment transaction, may be regarded as being very important. A credit card company or a bank can use an NFC card as personal ID and copy the identity or other information for such payment process.

An aspect of the applicant is a unique wearable identification device that may, e.g., be sold over jewelers or watch dealers worldwide. These jewelers and watch dealers have close links, and they provide an extra level of security.

The idea is to provide them with an after-sales link to the customer. And the customer gets an extra verification device for many applications (see elsewhere herein).

If someone copies the RFID identity, by reading and copying to an NFC chip, he cannot get access to the other information about the customer in the cloud, especially due to the described security measures. This information can only be accessed after entering additional information, especially security information.

The invention will now be further described with reference to the drawings.
Fig. 1 shows a piece of jewelry with a clasp,
Fig. 2 shows a first element,
Fig. 3 shows a second element,
Fig. 4 shows the clasp in a side view,
Fig. 5 shows an arrangement,
Fig. 6 shows an arrangement for performing a method,
Fig. 7 shows a flow diagram,
Fig. 8 shows a setting with a user and a tablet,
Fig. 9 shows a setting with a user and a shop,
Fig. 10 shows a second element, and
Fig. 11 shows a second element,

Fig. 12 to fig. 16 show a diagram of several processes, and
Fig. 17 shows a diagram of a payment process.

Fig. 1 shows a piece of jewelry 1 according to an embodiment. The piece of jewelry 1 comprises a chain 2 and a clasp 5 according to an embodiment.

The clasp 5 comprises a first element 10 which is further shown in fig. 2 and a second element 20 which is further shown in fig. 3. Both elements 10, 20 each comprise a respective magnetic element so as to attract each other in the position shown in fig. 1. These magnetic elements will be further described below.

The first element 10 comprises a main part 12, from which a protrusion 14 protrudes. The protrusion 14 has a cylindrical shape.

In addition, an arm 16 is secured to the main part 12. The arm 16 has a loop 18 with a hole 19 for securing the chain 2.

In detail, the first element 10 comprises a first magnetic element 15 that has a cylindrical shape and is made of a material like neodymium so as to be a permanent magnet. The first magnetic element 15 is secured in the main part 12 of the first element 10 and protrudes over the main part 12, so that it automatically forms the protrusion 14.

The second element 20 has a main part 22. In the main part 22, a clearance 24 is formed. The clearance 24 has a cylindrical shape. The aforementioned clearance 24 mates the protrusion 14, so that the elements 10, 20 may be put together such that the protrusion 14 is received in the clearance 24.

A second magnetic element 25 is positioned at the bottom of the clearance 24. Also, the second magnetic element 25 is made of a material like neodymium so as to be a permanent magnet.

The magnetic fields generated by the magnetic elements 15, 25 are such that they help to bring the first element 10 and the second element 20 in the correct orientation relative to each other when closing the clasp 5.

The second element 20 has a wall 21 encompassing a segment of a cylinder. When the first element 10 is in contact with the second element 20, this wall 21 partially surrounds the first element 10. This prevents an inadvertent contact with the first element 10 that could possibly disengage the first element 10 from the second element 20.

The second element 20 also has a loop 28 with a hole 29 for securing the chain 2.

The second element 20 has a gap 26 formed between the main part 22 and a cantilever 23. The cantilever 23 protrudes from the wall 21 and has a retaining element 27 at its free end.

The retaining element 27 is embodied as a sphere. Thus, it provides smooth surfaces in all directions downwards from the cantilever 23.

To secure the first element 10 to the second element 20 from a state in which both elements 10, 20 are separate from each other, the first element 10 can at first be inserted such that its protrusion 14 is received by the clearance 24. The arm 16 is positioned between the wall 21 and the cantilever 23 on the front side as shown in fig. 3. Especially, it does not yet engage the gap 26.

If the first element 10 is in a correct position relative to the second element 20, the two magnetic element 15, 25 provide for an attractive force between the elements 10, 20 so as to help the user during closing the clasp 5. If the position is incorrect, for example if the first element 10 is positioned at a bottom side of the second element 20, a guiding force is generated that helps the user to reach the correct relative position.

After the protrusion 14 has been received by the clearance 24, the first element 10 may be rotated relative to the second element 20 such that the arm 16 passes the

retaining element 27 under slight resilient deformation of the cantilever 23. After this operation, the arm 16 engages the gap 26. This corresponds to a closed state.

In order to release the first element 10 from the second element 20, the first element 10 may be rotated in the opposite direction under slight resilient deformation of the cantilever 23. Then, the arm 16 is again out of engagement with the gap 26 and the first element 10 can be separated from the second element 20.

Fig. 4 shows the clasp 5 in a side view in a closed state. The gap 26 that has already been described is clearly visible in this figure.

As shown, the arm 16 protrudes through the gap 26 and is secured in the gap 26 by the retaining element 27. This prevents an inadvertent release of the first element 10 from the second element 20.

If the arm 16 is turned to the left, it may slightly bend the cantilever 23 upwardly and may then be brought into a state in which the two elements 10, 20 can be released from each other. When bending the cantilever 23, it is of advantage that the retaining element 27 is embodied as a sphere, because the cantilever 23 can be smoothly bent resiliently upwards by the moving arm 16. The user will sense a certain resistance due to the retaining element 27. However, she will be able to overcome this resistance using human muscular force. As long as the clasp 5 should remain in a closed state, this resistance secures this closed state and prevents inadvertent release.

The first element 10 may be fabricated by taking a main part 12 having a cylindrical shape and processing it so as to form a cylindrical disc-shaped clearance. The first magnetic element 15 may be inserted into this clearance such that it protrudes out of the clearance, automatically forming the protrusion 14 due to its cylindrical shape. The arm 16 can be secured to the main part 12 using techniques like soldering or welding.

The second element 20 may be fabricated by taking a main part 22 having a cylindrical shape and processing it so as to form the clearance 24 also with a

cylindrical shape. The second magnetic element 25 may be inserted into the clearance 24. The second magnetic element 25 may partially fill the clearance 24, but leave an upper part of the clearance 24 so as to receive the protrusion 14 of the first element 10. The wall 21 may be processed separately such that it already comprises the cantilever 23. The retaining element 27 in the form of a sphere may be formed at the end of the cantilever 23. The wall 21 may then be secured to the main part 22 using techniques like soldering or welding. The loop 28 may also be secured by soldering or welding.

After fabrication of the first element 10 and the second element 20, the chain 2 may be attached to the loops 18, 28 in order to form the piece of jewelry 1, for example a necklace or bracelet.

Fig. 5 shows an arrangement 100 with which a method can be performed.

The arrangement comprises a network 106 with which several entities can communicate with each other. The network 106 may especially be the internet.

The arrangement 100 comprises several readout devices 108. These readout devices 108 may read out an identification number of an RFID tag. The RFID tag may be part of a wearable device, for example as described elsewhere herein.

The network 106 may communicate with a server 102 providing access to a database 104. The database 104 hosts data. The server 102 may read out data and store data and may further perform some operations like comparing data in order to determine if a user is authorized or not.

The readout devices 108 can thus be distributed worldwide and can access the database 104. The server 102 and the database 104 together may be denoted as a cloud storage system.

Fig. 6 shows an arrangement 200 for performing a method.

Several record-keeping units 202, 204, 206 are shown, which may be part of a database like the database 104 shown in fig. 5. Each record-keeping unit 202, 204, 206 may be controlled by a respective processor 210, 212, 214, each processor 210, 212, 214 communicating with a communications component 216. The communications component 216 may communicate with a processing unit 218, which may communicate with several RFID readers 220, 222, 224. The RFID readers 220, 222, 224 can readout data, for example an identification number, from an RFID tag being part of a wearable device.

Thus, data can be exchanged between the record-keeping units 202, 204, 206 and the RFID readers 220, 222, 224, for example in order to use an identification number stored in an RFID tag in order to identify a user and in order to retrieve user-related data stored in the record-keeping units 202, 204, 206.

Fig. 7 shows a flow diagram of a possible method 300. The method 300 may be performed by a cloud storage device, especially as shown in fig. 5.

The method 300 starts with receiving a tagging entry at step 302. The tagging entry is stored in a database in a step 304. Then location data is received in a step 306.

If it is determined in a step 308 that location data corresponds to the tagging entry, a further step 310 is performed in order to communication location data to an external entity. This location data can especially be used in order to verify an identity of a user.

Fig. 8 shows a user 30. The user 30 wears a wearable device 40. The wearable device 40 comprises an RFID tag on which an identification number is written. The RFID tag is a passive RFID tag that can be read out using specific radio waves.

The user 30 is, for example, sitting in a restaurant and wants to pay. For that purpose, the restaurant provides a tablet 50. The tablet 50 comprises an RFID reader 55 and a wireless communication device 57, which can also be denoted as an interface device.

The RFID reader 55 is able to read out the RFID tag of the wearable device 40. The wireless communication device 57 is able to connect to a wireless network in order to connect to the internet.

When the user wants to pay, he first brings his wearable device 40 in proximity to the RFID reader 55. The identification number stored in the RFID tag is read out and further processed by the tablet 50.

As payment information is required, additional security measures are implemented to ensure that only the owner of the wearable device 40 is able to perform a payment process.

The user is requested to select one of four kinds of security information:

FP: Fingerprint
FR: Face Recognition
VR: Voice Recording
PIN: PIN number

In the state shown in Fig. 8, the user may select one of the four alternatives. Afterwards, security information according to the selection is obtained. If fingerprint is selected, the user has to put his finger on a specific reader and the fingerprint is collected. If face recognition is selected, a picture is made from a face of the user. If voice recording is selected, a short speech of the user is recorded. If PIN number is selected, the user has to input a code.

The identification number together with the security information and a content of a variable defining the type “payment information” is transmitted in a request using the wireless communication device 57 to a cloud storage system. The cloud storage system is accessible using a standard internet connection.

The cloud storage receives the request, identifies the user using the identification number and verifies his identity using the security information. The security information is compared with stored reference information. If the user is verified, payment information is transmitted to the tablet 50, including credit card information,

for example. This payment information is then used in order to perform a payment process.

The same or a similar payment process may also be used at an ATM or other machine for retrieving money. It allows a user to desist from using a credit card or other payment means.

Fig. 9 shows a different setting. A user 30 wearing a wearable device 40 with an RFID tag stands in front of a store 60 having a readout device 65. If the user 30 enters the store 60, he holds his wearable device 40 near the readout device 65. The readout device 65 reads the identification number out of the RFID tag and sends a request comprising this identification number and a content of a variable having the type “personal preference information” to the cloud storage system. The cloud storage system sends preference information back. This information is presented on a screen to the shop owner immediately when the user 30 enters the store 60.

Thus, the shop owner or shop employee knows about the user’s preferences, for example colors or materials, and thus can decide which products to offer.

In an alternative implementation, a restaurant can apply the implementation instead of a shop 60. The restaurant thus may know about personal preferences of the user 30. For example, the restaurant can be informed if the user likes big macs or cheeseburgers. For example, the restaurant can also be informed about food allergies or religious exclusions of specific food.

In an additional or alternative implementation, the RFID tag of the wearable device 40 may be used for inventory control before selling the wearable device. For example, a company may write an inventory control number in the RFID tag and may read it out each time an inventory should be controlled. Especially, each wearable device may be tracked prior to sale. During or after sale, the inventory control number can be replaced by the identification number, or the inventory control number can be used as the identification number.

When the identification number is processed in a cloud storage system, the cloud storage system may identify if the identification number corresponds to a stored reference. If no reference should be found, the wearable device from which the identification number was read out may be identified as potentially being subject to forgery.

The cloud storage system may also store indications that a wearable device has been stolen. If the cloud storage system finds out that a dataset corresponding to an identification number indicates that the wearable device having this identification number has been stolen, it may, for example, deactivate further use of this identification number and/or inform a police or owner using predetermined contact data.

The identification number may also be used in order to provide an electronic invoice to a customer. For example, an electronic invoice can be stored with relation to an identification number, and when the identification number is read out the electronic invoice may be provided, for example to a predefined e-mail address.

The identification number may also be used in order to provide an electronic warranty card to a customer. For example, an electronic warranty card can be stored with relation to an identification number and when the identification number is read out the electronic warranty card may be provided, for example to a predefined e-mail address.

The identification number may also be used in order to provide an electronic product information to a customer. For example, an electronic product information can be stored with relation to an identification number, and when the identification number is read out the electronic product information may be provided, for example to a predefined e-mail address.

Fig. 10 shows a second element 20 as a part of a clasp 5 being a wearable device that can be used for identification purposes. The second element 20 houses an RFID tag 70. The RFID tag 70 has, in the shown embodiment, a cuboid shape and a cross section with outer dimensions of approximately 2 mm x 2 mm.

Fig 11 shows a second element 20 with an RFID tag 70 according to a different implementation. In this implementation, an antenna 75 is provided as a part of the RFID tag 70.

It should be noted that even if some features or method steps have been disclosed in combination, a person skilled in the art will recognize that they can also be used or performed separately and can be combined with other features or method steps disclosed herein, regardless of whether they have been disclosed separately or together with other features or method steps.

Figs. 12 to 16 show a diagram showing different aspects of a use of an RFID device and especially of a clasp system. Connections between the figures are shown in rectangular surroundings.

In fig. 12, steps that may be performed by a manufacturer are shown. In step 1, a manufacturer may request for an RFID number from HQ, wherein HQ is a central software system, commonly operated as a cloud storage system. The system may record an RFID number that has been issued to a manufacturer. Especially, the RFID number may be sent via e-mail.

In step 2, the manufacturer may update a system with a product tag. This may especially be used for inventory control by the manufacturer. Thus, the manufacturer has always a control regarding his inventory of clasps.

In step 3, the manufacturer may pass the product to a company. The company can change the RFID or the content of the RFID via the main system, which may especially be the HQ. The RFID lock may be created at a backend.

In a further step, an RFID code may be encrypted. This can prevent an unauthorized readout.

For example, a 16 number RFID code can be used, wherein the example 1111-2222-3333-4444 is shown in fig. 12. The first four digits may indicate a running ID. This can

be used in order to identify a specific clasp. The fifth to eighth digits can be used in order to identify a manufacturer, a company, or a retailer. The ninth to twelfth digits may be used in order to identify a product. The last four digits may be used in order to identify a customer.

After steps performed by the manufacturer, further steps may be performed by a retailer having onboarding customers, or by customers themselves. This is shown in figs. 13 and 14.

In step 1, an admin may be registered on a system based on the number stored in the RFID tag. The tag may especially be present in a jewel, an accessory, or a watch (together abbreviated as JAW). A product description may be registered at the system. An inventory or other stock management system may be updated.

In step 2, a customer may register upon purchase. An admin may register customer details via the system. The tag has an RFID and is typically inserted in a JAW product. In step 2.1, the customer may be required to present an ID card and/or a passport, wherein such identification means can be used regardless of the specific country in which the customer resides.

In step 2.2, security measures are implemented. They may be called 4FA, because four types of security measures may be implemented, as has been described elsewhere herein.

In step 2.3, a customer personal ID number may be generated. In step 2.4, the RFID may be rewritten with the personal ID number. The personal ID number may especially be used as identification number as described elsewhere herein. In step 2.5, the personal ID may be encrypted. In step 2.6, a warranty card may be tagged to the product, an electronic invoice may be tagged to the product, and a portfolio or collection may be added.

In step 3, the customer may download a corresponding clasp mobile app. Personal details may be filled in, for example a medical report, which may be secured with security measures according to a level 2 information. Thus, readout of medical data

by unauthorized persons may be prevented. Records of JAW and RFID may be shown in order to generate a purchase portfolio. In addition, payment details may be saved, wherein such payment details are optional features. The 4FA security features may be applied by the admin via the system. Especially, facial recognition, voice recognition, a pin code and/or fingerprint may be used for increased security. A customer can import a company profile with image and YouTube link. This can increase information about the customer so that he may be identified and he may present himself with his corporate profile. The customer profile may also include hobbies, as such hobbies can, for example, be used in order to start a conversation with someone else having the same hobbies, even if the customer did not know the person before. The customer can select what he is looking for, for example by entering details such as product categories, color, and materials. This can even be done without a product catalog. The customer can input personal details such as food allergies, favorite drinks, or health record, which can, for example, be used in a restaurant in order to allow a waiter to know which food or drinks to offer.

A loss or theft of the clasp may be reported. In step 1, the customer may log in the mobile app. He may select his lost JAW product in step 2. In step 3, he may report the loss or theft. In step 4, providers can be notified. In step 5, the customer can be notified via mobile app when the item was found by the admin or by any other person. For example, police or dealers may be informed about the lost or stolen item so that they can report it to the system when a product with a specific identity read out from the RFID tag was found.

The clasp may be used for a meet and greet functionality. This is shown in figs. 15 and 16.

In step 1, a customer may allow a meet and greet function, for example via the already mentioned mobile app. People meet and greet, shop meet and greet, and dining meet and greet can be allowed or disallowed separately.

In step 2, an organizer of an event or another person may activate an organizer app. This may allow customers to scan their RFID. In addition, a QR code may be scanned via the mobile app, so that a profile may be loaded. A tag with an event ID,

which can be valid until an event end time, may be generated in order to identify a specific event.

In step 3, a customer may check in, for example in a shop, retrieving “meet and greet” information and can notify an admin via the system about a customer arrival. The admin can view a profile and preferences of the customer. People in a shop may be notified. A public profile may be used in order to connect. A user can send greetings via text, virtual name cards, and voice. A user can choose to follow a friend and will receive notifications if the friend is in the same shop.

In step 4, a kiosk can be provided for customer quick view. The RFID may be scanned, and/or a QR-code may be scanned via the mobile app. The availabilities of the items in a wish list of the customer may be viewed.

Especially, there may be three types of meet and greet. A first type may be at a conference or other event. The second type may be in a shop. The third type may be while dining, especially in a restaurant. There may be provided an additional user interface, for example for a shop attendee and/or for a dining attendee, to record data of a customer such as favorite drinks and foods, to store purchase records, and in order to use a tablet app. The tablet app can, for example, be provided to a customer in order to perform identification and/or payment functions.

A possible payment process is shown in fig. 17. In step 1, the customer may allow the RFID payment mode via a mobile application. The customer may input payment details. The customer may especially be required to do a verification with an admin. For example, a personal ID or a passport may be used for such verification.

In step 2, the RFID or QR-code may be scanned via the mobile app on an admin system. The admin may input a shopping cart, for example a bill of a restaurant in which the user was dining. The admin may start the payment process. The customer can verify, for example via two security features using the admin device. For example, facial recognition and expression recognition may be used. Alternatively, or additionally, voice recognition with tonality recognition may be used. Alternatively, or additionally, a fingerprint may be scanned and used for safety purposes.

Alternatively, or additionally, a pin-code can be used. The mode of payment may be decided upon registration. For example, a price level can be used in order to decide on the mode, or in order to exclude some modes. For example, if a price to be paid is above a certain limit, some less secure payment modes may be deactivated.

In step 3, the payment may be completed. Thus, the customer can use his JAW product, for example a clasp, with an RFID tag for payment. Respective information may be kept as records in the system.

In the following, certain features are provided in a structured form.

1. Method for retrieving user-related data from a cloud storage system, the method comprising the following steps:
- reading out an identification number from an RFID tag,
- providing a variable, a content of the variable indicating a type of user-related data using an interface device,
- sending a request comprising the identification number and the type to the cloud storage system, especially using the interface device, and
- receiving user-related data from the cloud storage system, the user-related data especially being based on the identification number and the content of the variable.

2. Method according to item 1,
- wherein the content of the variable and/or the type is provided by a device performing the method.

3. Method according to one of the preceding items,
- wherein the content of the variable and/or the type is provided by user input.

4. Method according to one of the preceding items,
- wherein, when the type is out of a first group of types, only the identification number and the type are sent to the cloud storage system.

5. Method according to one of the preceding items,
- wherein, when the type is out of a second group of types, at least one security information is obtained and is sent in addition to the identification number and the type to the cloud storage system.

6. Method according to item 5,
- wherein obtaining security information comprises taking a fingerprint, and
- wherein the security information comprises information regarding the fingerprint.

7. Method according to one of items 5 or 6,
- wherein obtaining security information comprises taking a speech record, and
- wherein the security information comprises information regarding the speech record.

8. Method according to one of items 5 to 7,
- wherein obtaining security information comprises taking a picture of a face, and
- wherein the security information comprises information regarding the picture of a face.

9. Method according to one of items 5 to 8,
- wherein obtaining security information comprises inputting a code, and
- wherein the security information comprises information regarding the code.

10. Method according to one of the preceding items,
- wherein one type is ownership information;
and/or
- wherein one type is medical information;
and/or
- wherein one type is meet and greet information;
and/or
- wherein one type is personal preference information;
and/or
- wherein one type is payment information.

11. Method according to one of the preceding items,
- wherein the received user-related data is presented on a screen of a device preforming the method.

12. Method according to one of the preceding items,
- wherein the method is performed in a mobile electronic device, a tablet, or a stationary electronic device.

13. Method according to one of the preceding items,
- wherein the RFID tag is a passive RFID tag.

14. Method for performing a payment process,
the method comprising the following steps:
- reading out an identification number from an RFID tag secured in a wearable device,
- setting a content of a variable for defining a type of user-related data to be payment data,
- requesting security information,
- obtaining security information,
- sending a request comprising the identification number, the content of the variable and the security information to a cloud storage system,
- receiving user-related data being payment data from the cloud storage system, and
- performing the payment process using the payment data.

15. Method according to item 14,
- wherein the security information is a fingerprint, a voice record, a picture of a face, or a code.

16. Method according to one of items 14 or 15,
further comprising a step of
- selecting which kind of security information should be requested.

17. Method according to item 16,
- wherein the selecting is performed by user input.

18. Method according to one of items 16 or 17,
- wherein selecting is performed automatically based on an amount to be paid, a location, a venue, and/or based on other information.

19. Method for providing user-related information to a person,
the method comprising the following steps:
- reading out an identification number from an RFID tag secured in a wearable device,
- setting a content of a variable for defining a type of user-related data to be meet and greet information or personal information,
- sending a request comprising the identification number and the content of the variable to the cloud storage system,
- receiving user-related data from a cloud storage system, and
- presenting the user-related data on a display and/or sending the user related data to another electronic device.

20. Readout device, comprising
- an RFID reader being configured to read out an identification number from an RFID tag, and
- an interface device being configured for
  - providing a content of a variable indicating a type of user-related data using an interface device,
  - sending a request comprising the identification number and the content of the variable to a cloud storage system, and
  - receiving user-related data from the cloud storage system, the user-related data preferably being based on the identification number and the content of the variable.

21. Readout device, comprising
- an RFID reader and an interface device,
- the readout device being configured to perform a method according to one of items 1 to 19.

22. Cloud storage system, the cloud storage system being configured to
- receive a request comprising an identification number and a content of a variable indicating a type of user-related data, and
- send user-related data depending on the identification number and the content of the variable.

23. Cloud storage system according to item 22,
- being further configured to receive security information, to compare the security information with stored reference data, and to send user-related data only if the security information corresponds to the stored reference data.

24. Method for inventory control of a personal identification device,
the method comprising the following steps:
- writing an inventory control number in an RFID tag, and
- tracking the personal identification device using the inventory control number.

25. Method according to item 24,
- wherein the inventory control number is read out from the RFID tag each time an inventory should be determined.

26. Method for forgery control and/or theft control of a wearable device,
the method comprising the following steps:
- reading out an identification number from an RFID tag of the wearable device,
- comparing the identification number to a reference dataset, and
- indicating forgery if the identification number does not correspond to the reference dataset, or indicating theft it the reference dataset indicates that the identification number corresponds to a stolen device.

27. Method for providing an electronic invoice for a wearable device,
the method comprising the following steps:
- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to an invoice system, and
- providing an electronic invoice by the invoice system based on the identification number.

28. Method for providing an electronic warranty card for a wearable device,
the method comprising the following steps:
- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to a warranty system, and

- providing an electronic warranty card by the warranty system based on the identification number.

29. Method for providing an electronic product information for a wearable device, the method comprising the following steps:
- reading out an identification number from an RFID tag of the wearable device,
- sending the identification number to a product information system, and
- providing an electronic product information by the product information system based on the identification number.

30. Personal identification device, comprising
- a tag holder for mechanical connection with a wearable device (20), and
- an RFID tag being mechanically connected with the tag holder,
- wherein the RFID tag has stored, or is configured to store, an identification number.

31. Personal identification device according to item 30.
- wherein the tag holder is fully or partially made of a precious metal.

32. Personal identification device according to one of items 30 or 31,
- wherein the RFID tag has a round shape.

33. Personal identification device according to one of items 30 to 32,
- wherein the RFID tag has a diameter of at least 1 mm and/or of at most 4 mm.

34. Personal identification device according to one of items 30 to 33,
- wherein the RFID tag has a diameter of 1.5 mm or 3 mm.

35. Personal identification device according to one of items 30 to 34,
- wherein the tag holder forms an antenna or an antenna amplifier for the RFID tag.

36. Wearable device (20), comprising
- a fastening structure for fastening the wearable device (20) to a human body, and
- a personal identification device according to one of items 20 to 25.

37. Wearable device (20) according to item 36,
- wherein the wearable device (20) is a mechanical watch.

38. Wearable device (20) according to one of items 36 or 37,
- wherein the wearable device (20) is a piece of jewelry.

39. Wearable device (20) according to one of items 36 to 38,
- wherein the wearable device (20) is a clasp.

40. Wearable device (20) according to one of items 36 to 39,
- wherein the tag holder is soldered or lasered in the wearable device (20).

List of reference signs:

1	piece of jewelry
2	chain
5	clasp
10	first element
12	main part
14	protrusion
15	first magnetic element
16	arm
18	loop
19	hole
20	second element
21	wall
22	main part
23	cantilever
24	clearance
25	second magnetic element
26	gap
27	retaining element / sphere
28	loop
29	hole
30	user
40	wearable device
50	tablet
55	RFID reader
57	wireless communication device
60	store
65	readout device
70	RFID tag
75	antenna
100	arrangement
102	server
104	database
106	network

108 readout device

200 arrangement

202, 204, 206 record-keeping unit

210, 212, 214 processor

216 communications component

218 processing unit

220 RFID reader

300 method

302 - 310 steps

Claims

1. Clasp (5), comprising
- a first element (10), and
- a second element (20),
- wherein the first element (10) has a protrusion (14), and the second element (20) has a clearance (24) for receiving the protrusion (14) of the first element (10) such that the first element (10) is rotatable with respect to the second element (20),
- wherein the first element (10) has an arm (16), and the second element (20) has a gap (26), wherein the arm (16) engages the gap (26) when the first element (10) is rotated with respect to the second element (20) into a closed state,
- wherein the first element (10) is removable from the second element (20) when the arm (16) does not engage the gap (26).

2. Clasp (5) according to claim 1,
- wherein the protrusion (14) has a circular cross section.

3. Clasp (5) according to one of the preceding claims,
- wherein the clearance (24) has a circular cross section.

4. Clasp (5) according to one of the preceding claims,
- wherein the clearance (24) mates the protrusion (14).

5. Clasp (5) according to one of the preceding claims,
- wherein the gap (26) is defined between a cantilever (23) and a main part (22) of the second element (20).

6. Clasp (5) according to one of the preceding claims,
- wherein the gap (26) has, at an end at which the arm (16) enters the gap (26) from an open state, a retaining element (27), the retaining element (27) releasably retaining the arm (16) in the gap (26).

7. Clasp (5) according to claim 6,
- wherein the retaining element (27) is embodied as a sphere partially closing an entry of the gap (26).

8. Clasp (5) according to claim 5 and one of claims 6 or 7,
- wherein the retaining element (27) is positioned at a free end of the cantilever (23).

9. Clasp (5) according to one of the preceding claims,
- wherein the first element (10) is not removable from the second element (20) when the arm (16) engages the gap (26).

10. Clasp (5) according to one of the preceding claims,
- wherein the first element (10) has a first loop (18) with a first hole (19) for securing another element,
and/or
- wherein the second element (20) has a second loop (28) with a second hole (29) for securing another element.

11. Clasp (5) according to one of the preceding claims,
- wherein the first element (10) and/or the second element (20) comprise a magnetic element (15, 25) so as to attract each other by magnetic force.

12. Clasp (5) according to claim 11,
- wherein the first element (10) comprises a first magnetic element (15) forming the protrusion (14).

13. Clasp (5) according to one of claims 11 or 12,
- wherein the second element (20) comprises a second magnetic element (25) being positioned in the clearance (24).

14. Clasp (5) according to one of the preceding claims,
- wherein the first element (10) and/or the second element (20) are fully or partly made of gold, silver, metal, or metal alloy.

15. Clasp (5) according to one of the preceding claims,
- wherein the second element (20) has a wall (21) encompassing a segment of a circle and laterally securing the first element (10) when the protrusion (14) is received in the clearance (24).

16. Clasp (5) according to one of the preceding claims,
- further comprising an identification tag in the first element (10), the second element (20), or between the first element (10) and the second element (20).

17. Piece of jewelry (1), especially necklace or bracelet, comprising a clasp (5) according to one of the preceding claims.

18. Piece of jewelry (1) according to claim 17, comprising at least one chain (2) being attached to the first element (10) and/or to the second element (20) of the clasp (5).