Appeal decision

Appeal No. 2019-5292

Appellant	Arm IP Limited
Patent Attorney	ONO, Makoto
Patent Attorney	KANAYAMA, Masakata
Patent Attorney	TSUBOKURA, Michiaki
Patent Attorney	SHIGEMORI, Kazuki
Patent Attorney	ANDO, Kenshi
Patent Attorney	ICHIKAWA, Hidehiko
Patent Attorney	AOKI, Takahiro
Patent Attorney	SAKURADA, Yoshie
Patent Attorney	KAWASAKI, Yosuke
Patent Attorney	GOMIBUCHI, Takuya
Patent Attorney	KONDO, Toshikazu
Patent Attorney	IINO, Yoichi
Patent Attorney	ICHIKAWA, Yusuke
Patent Attorney	MORIYAMA, Masahiro
Patent Attorney	IWASE, Yoshikazu

Patent Attorney SHIROYAMA, Yasufumi

The case of appeal against the examiner's decision of refusal of Japanese Patent Application No. 2016-520737, entitled "Trusted Device" (International publication on December 24, 2014, WO2014/202951, Domestic publication on August 12, 2016, National Publication of International Patent Application No. 2016-524249) has resulted in the following appeal decision.

Conclusion

The appeal of the case was groundless.

Reason

No. 1. History of the procedures

The application was filed on June 9, 2014 as an international filing date (Priority Claim received by the foreign receiving office under the Paris Convention on June 18, 2013, US).

A translation written into Japanese of the specification, claims, and drawings (only description in drawings) in accordance with the provisions of Article 184(4)(i) of the Patent Act was submitted on February 10, 2016, a request for examination was filed on March 15, 2017, a notice of reasons for refusal was issued by the examiner on December 25, 2017, and although, a written opinion and written amendment were submitted on July 4, 2018. However, a decision of refusal was issued by the examiner on December 14, 2018. Against this, a request for appeal and a written amendment were submitted on April 22, 2019, and a report based on the provisions of Article 164(3) of the Patent Act was issued by the examiner on June 26, 2019.

No. 2. Regarding the invention

The invention relating to Claim 1 of the present application (hereinafter referred to as the "Invention") is acknowledged as follows, as specified by the matters described in Claim 1 according to the scope of claims for patent amended by the written amendment submitted on April 22, 2019.

"A trusted device comprising:

authentication circuitry configured to authenticate with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring circuitry configured to monitor physical possession of said trusted device by said user following said authentication operation and to switch said trusted device out of said authenticated state if said trusted device is not in physical possession of said user, said retention monitoring circuit being equipped with one or more detection circuits including a photo-detector shielded from light when said trusted device is physical possession of said user;

communication triggering circuitry configured to detect a request to establish communication received from a target device that is one of a plurality of different target devices; and

communication circuitry configured to communicate with said target device if said trusted device is in the authenticated state".

No. 3. Reasons for refusal stated in the examiner's decision

The reasons for refusal that were grounds for the decision of refusal dated December 14, 2018 in the original examination (hereinafter, referred to as "the decision of refusal of the original examination") are that

1. The invention according to Claim 1 of the case could have been easily made by a person ordinarily skilled in the art of the inventions before the priority date, on the basis of the inventions described in Cited Document 1 to Cited Document 4 which had been distributed or available to public over an electric communication network in Japan or a foreign country before the priority date of the present application (hereinafter referred to as "the priority date") and on the well-known art described in Cited Document 5. Therefore, the Appellant should not be granted a patent for it under the provisions of Article 29(2) of the Patent Act.

<Cited Documents>

1. National Publication of International Patent Application No. 2005-538430
2. National Publication of International Patent Application No. 2005-528662
3. Japanese Unexamined Patent Application Publication No. 2004-280245
4. International Publication No. 2009/028018
5. Japanese Unexamined Patent Application Publication No. 2001-195145

2. The description of Claim 3 of the present application does not comply with the requirements under Article 36(6)(ii) of the Patent Act in the following point.

Note

<Remainder omitted>

No. 4. Matters described in Cited Documents

1. National Publication of International Patent Application No. 2005-538430 (published on December 15, 2005, hereinafter, referred to as "Cited Document 1") that was cited in the reasons for refusal dated December 25, 2017 in the original examination (hereinafter, referred to as "the reasons for refusal of the original examination") and had already been publicly known before the filing of the present application in the first country describes the following matters together with the related drawings.

A. "[0005]

[SUMMARY OF THE INVENTION]

A method and versatile device for use-based context security is described and provided. In an embodiment, the versatile device is implemented as a wristwatch. The wristwatch is configured to facilitate a wireless transaction for an authenticated user and is configured to be worn by the authenticated user so as to encircle a part of the authenticated user. The wireless transaction may be of any type (e.g., credit card type, debit card type, access control type, etc.). Moreover, the wristwatch includes a validation mechanism for controlling use of the wristwatch based on whether or not the authenticated user continues to wear the wristwatch after initiating use of the wristwatch.

[0006]

In particular, the wristwatch executes a context security validation scheme, where authenticated use is determined not only by possession of the wristwatch, but also by its operational context. The operational context will allow the wristwatch to accept or deny any external service interaction via a wireless link, based on whether the wristwatch is in an active/secure status state or in an inactive state. Moreover, the integration of a data channel within the straps of the wristwatch itself enables validation of whether or not the wristwatch is being worn by the authenticated user that initiated use of the wristwatch. Removal of the wristwatch will invalidate its context security and place the wristwatch in an inactive state, disabling all external interaction via the wireless link". (Underlines were added for convenience of description by the body. The same shall apply hereinafter.)

B. "[0013]

FIG. 1 illustrates a wristwatch 100 in accordance with an embodiment of the

present invention. The versatile device 100 of the present invention is configured to be worn by an authenticated user so as to encircle a part of the authenticated user's body. In an embodiment, the versatile device 100 is implemented as a wristwatch 100 as shown in FIG. 1. Alternatively, the versatile device 100 may be implemented as any finger, hand, arm, foot, leg, waist, wrist, or other body worn item, such as a bracelet or armband. It should be understood that the wristwatch 100 may have other configurations.

[0014]

In particular, the wristwatch 100 includes an electronic circuitry 50 to host one or more applications, secure authentication/identification data, and transaction data, and to validate use and possession of the wristwatch 100 by a legitimate user by executing a use-based context security validation scheme. The wristwatch 100 is configured to facilitate a wireless transaction for an authenticated user and is configured to be worn by the authenticated user so as to encircle a part of the authenticated user, such as the authenticated user's wrist. The wireless transaction may be of any type (e.g., credit card type, debit card type, access control type, etc.). Moreover, the wristwatch 100 includes a validation mechanism for controlling use of the wristwatch 100 based on whether or not the authenticated user continues to wear the wristwatch 100 after initiating use of the wristwatch 100. The validation mechanism includes a transmitting element 40, a receiving element 30, a data channel 80, and a monitoring component (integrated in the electronic circuitry 50) for monitoring the status of the data channel 80.

[0015]

Moreover, the wristwatch 100 executes a context security validation scheme, where authenticated use is determined not only by possession of the wristwatch 100, but also by its operational context. According to the operational context, the wristwatch 100 will be allowed to accept or deny any external service interaction via a wireless link, based on whether the wristwatch 100 is in an active/secure status state or in an inactive state. In particular, the wristwatch 100 integrates a data channel 80 within the first and second straps 10 and 20 of the wristwatch 100 itself enabling validation of whether or not the wristwatch 100 is being worn by the authenticated user that initiated use of the wristwatch 100. Removal of the wristwatch 100 will invalidate its context security and place the wristwatch in an inactive state, disabling all external interaction via the wireless link."

C. "[0018]

As illustrated in FIG. 1, the wristwatch body 90 acts as the main functional

section. The wristwatch body 90 provides time and date functions via the watchface 60. Moreover, the wristwatch body 90 provides secure data storage capability, wireless transaction capability, and an encryption engine for the validation mechanism. Moreover, the wristwatch 100 integrates a data channel 80 within the first and second straps 10 and 20 of the wristwatch 100 itself enabling validation of whether or not the wristwatch 100 is being worn by the authenticated user that initiated use of the wristwatch 100. The wristwatch body 90 includes an embedded electronics subsystem 50, a transmitting element 40 for transmitting data through the data channel 80, a receiving element 30 for receiving the data transmitted through the data channel 80, and optional biosensors 70 for sensing whether or not the authenticated user is wearing the wristwatch 100. A successful transmission of the data between the transmitting element 40 and the receiving element 30 indicates that the wristwatch 100 is being worn by the authenticated user. Moreover, the data channel 80 is configured to be rendered inoperable if the authenticated user discontinues wearing the wristwatch 100. Specifically, the data transmitted by the transmitting element 40 are transmitted periodically and are time-varying to avoid unauthorized interference by monitoring the integrity and status of the data channel 80. In particular, the encryption engine facilitates secure transmission of the data through the data channel 80. In addition, the wristwatch 100 includes a clasp or strap connection mechanism 85".

D. "[0020]

The wristwatch 100 is capable of providing a low cost and robust authentication solution by ensuring the integrity of the data channel 80 integrated into the first and second straps 10 and 20. Security can be enhanced by using the optional biosensor subsystems 70 and 71, providing the capability to detect the presence or absence of the authenticated user's body using biometric measurement techniques (e.g., skin temperature, light reflection, humidity), in addition to the integrity of the data channel 80 itself.

[0021]

FIG. 3 illustrates a flow chart showing a method 300 of securely operating the wristwatch 100 of FIG. 1 in accordance with an embodiment of the present invention. Reference is made to FIG. 1 and FIG. 2.

[0022]

In Step 310, a user wears the wristwatch 100. Moreover, in Step 320, the user goes through a security initialization procedure to authenticate the user prior to allowing the user general operational use of application hosting functionality of the wristwatch

100 to facilitate a variety of wireless transactions for the authenticated user. The initialization procedure may be a simple wristwatch-based operation (e.g. entering a PIN number on the wristwatch itself) or a more complex security procedure involving an external security system in Step 325 (e.g. an external device with retina scanning hardware could be used to provide unique user verification, which is conveyed to the wristwatch 100 via the encrypted RF data communications link 302). Whatever the chosen initialization method, its task is to activate authenticated use of the wristwatch 100 by validating both the user and the data channel 80 integrated into the straps of the wristwatch 100. If the optional bio-sensing subsystem 70 is used, the initialization process will also validate the presence of the user's body.

[0023]

Once the user is authenticated, the wristwatch 100 enters an active/secure status state (in Step 330) and starts execution (in Step 370) of one or more applications, which are configured to facilitate wireless transactions and services. The wireless transaction and services may be of any type (e.g., credit card type, debit card type, access control type, etc.).

[0024]

In Step 375, when the wristwatch 100 is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch 100, the particular application checks in Step 380 whether or not the wristwatch 100 is operating in the active/secure status state. If the wristwatch 100 is not operating in the active/secure status state, the particular application denies the user access to the particular application in Step 390. If it is operating, the particular application then checks in Step 385 the validity of the interrogation (e.g., whether or not the user has subscribed to the particular service, and whether or not the user has paid the bill for the particular service). If the interrogation is not valid, the particular application denies the user access to the services offered by the particular application in Step 390. If it is valid, in Step 395, the particular application executes the desired service or transaction supported by the particular application.

[0025]

In Steps 335, 340, 345, 350, and 355, the integrity of the data channel 80 integrated into the straps is monitored. In particular, at periodic intervals, data are transmitted to the data channel 80 to validate the active/secure status state of the wristwatch 100. By transmitting and receiving a time varying encrypted data packet, the data channel 80 becomes more secure against attack or eavesdropping. The

validation process uses its own data for transmission through the data channel 80, independent from the hosted applications or secure data stored in the wristwatch 100.
[0026]

If a change in the active/secure status state is detected in Step 350 because the data channel has become inoperable indicating that the authenticated user has removed the wristwatch 100, the wristwatch 100 erases (in Step 360) its active/secure status state and application data and then switches (in Step 365) to an inactive state or off. Once switched off, others cannot use the wristwatch 100 to execute services or transactions. Once switched off, the wristwatch 100 can only be re-activated by the user after wearing the wristwatch 100 and re-performing the initialization procedure described above. The optional bio-sensing subsystem (in Step 340) provides an extra level of security by determining the user's presence as a supplement to the monitoring of the status and integrity of the data channel 80. Abnormal changes detected by the biosensors will result in the performance of the operations in Steps 360 and 365 as described above".

E. "[0027]

FIG. 4 illustrates a wristwatch 400 in accordance with another embodiment of the present invention, showing optical data channels 480A and 480B. The wristwatch 400 includes a first and a second plastic strap 450 and 451 and a buckle fastener 485. In an embodiment, the buckle fastener 485 is typical of those used on the most low-cost watches. Each strap 454 and 450 is manufactured so that the optical light paths 480A and 480B are integrated. The optical light paths 480A and 480B form the optical data channel of the wristwatch 400. This may be achieved by embedding an optical fiber in each strap. Alternatively, this may be achieved by manufacturing each strap from materials that possess appropriate optical properties".

2. National Publication of International Patent Application No. 2005-528662 (published on September 22, 2005, hereinafter, referred to as "Cited Document 2") that was cited in the reasons for refusal of the original examination and had already been publicly known before the filing of the present application in the first country describes the following matters together with the related drawings.

F. "[0023]

This embodiment of the present invention presents a device that enables a completely contact free SmartCard transaction that benefits from the high security of

biometric data comparison and verification yet allows for extremely convenient transactions. In the implementation of the embodiment envisioned, the SmartCard chip is contained in a wearable piece of functional jewelry; in this implementation, a wristwatch. This implementation, which could carry a possible trade name of 'AuthentiSwatch' and will be referred to as such in much of this discussion, houses not only the SmartCard electronic circuits, but also a transceiver device that also provides a biometric data reader. Further discussion of some of the embodiments of the present invention can be aided by reference to the figures. Note that, while this discussion focuses on the implementation of this embodiment as a timepiece, many other implementations are envisioned, including wearable security badges, broaches, and possibly tie pins, cufflinks, belt buckles or even writing pens or PDA styli.

[0024]

FIG. 1 illustrates a possible implementation of one embodiment of the present invention. In FIG. 1, 'AuthentiSwatch' 100 is enabled with a time/date display 101, a wrist band 102, an adjustment knob 103, and a display area 104 which is shown here with a latitude and longitude display from a GPS receiver. Also shown is an area 105, which is enabled in this implementation as a fingerprint scanner, and a bezel ring 106. The bezel ring 106 is shown only to illustrate the possibility of implementing an input device, perhaps to enable input of a PIN or to select a function from several. An item 107 is strictly for illustrative purposes. It is included to illustrate the ease of including infrared or RF communication in the watch body in order to implement non-contact communication.

[0025]

Each of the items shown in FIG. 1 is only included for the purpose of illustration and example. None of the features illustrated should be construed as being an intrinsic part of this embodiment. Not shown in the illustration but understood to be fully implemented is the SmartCard chip at the heart of this embodiment.

[0026]

The SmartCard chip would be, in this implementation, the residence of the biometric data employed with fingerprint scanner 105. In one envisioned enablement, the user would touch the proper finger to the fingerprint scanner, and a proper authentication coupled with proximate communication would result in a valid user verification.

[0027]

In another envisioned embodiment, a sensor of the proper type is implemented on the back of watch 100 that could read body temperature or perhaps vein patterns on

the wearer's wrist. In this fashion, yet another layer of biometric data security could be implemented in the same device. In one possible implementation of a wrist-worn embodiment, the device could be disabled until it is properly worn by a correct user, even if a correct fingerprint were read. This additional security layer might provide yet another disincentive to theft. Other, alternative, biometric input that could be implemented might be speech pattern recognition or perhaps an iris image."

G. "[0030]

The range of applications of wireless transactions has no discernible limit. However, a few exemplary applications are outlined here in order to fully discuss this embodiment of the present invention. FIG. 3 illustrates the application of this embodiment of the present invention as an e-cash device. In FIG. 3, the user is paying for a store-bought purchase by the use of his e-cash SmartCard enabled AuthentiSwatch, 100. The counterpart electronic wireless transaction apparatus is a vending device 300.
[0031]

In the embodiment of the present invention shown in FIG. 4, the enabled transaction is a public parking meter at a car parking facility. The parking meter is enabled by a counterpart transaction device 400 to communicate wirelessly with the AuthentiSwatch 100. Since it is envisioned that the wireless communication associated with this embodiment of the present invention is of a short range type, proximity to an enabled parking meter may serve in this scenario to select the desired transaction. Authentication would then be sent by the user's biometric data reader activation. It is possible that this activation could be initiated by the user's touching of a fingerprint reader.
[0032]

FIG. 5 illustrates another, slightly different type of transaction. Here, the user is assumably an authorized person seeking entry into a restricted entry area. By activating the biometric data reader on the AuthentiSwatch 100, the user could transmit his or her identity to a counterpart device 500 adjacent to a secure door, 510. The security system associated with the secured area would then make a determination as to whether or not the validly identified user is an authorized person."

3. Japanese Unexamined Patent Application Publication No. 2001-195145 (published on July 19, 2001, hereinafter, referred to as the "Well-known literature") that was shown for illustrating a well-known art in the decision of refusal of the original examination and had already been publicly known before the filing of the present application in the

first country describes the following matters together with the related drawings.

H. "[0012]
[Embodiments of the invention] An information processor, a personal authentication method, and a computer-readable recording medium on which a program for executing the method by a computer is recorded will be described as a preferred embodiment of the present invention with reference to the accompanying drawings in detail.
(Configuration of Information Processing System) FIG. 1 is a diagram showing the configuration of an example of a personal authentication system including an information processor in this embodiment. The system shown in FIG. 1 is constituted by an external unit (personal computer) 100 and an information processor (wristwatch type of information processor) 101.
[0013] The external unit 100 may be any of systems requiring authentication before use, for example, a personal computer, a portable telephone, a PDA, a lock mechanism and system for opening and closing a door, a personal safe, a briefcase, a pocketbook, etc., a mechanism and system for on/off control of main power source of various electrical systems, a system for controlling a household electrical appliance, or a lock mechanism and system for opening and closing a door, a trunk, or a fuel tank cap of automobile.
[0014] The information processor (wristwatch type of information processor) 101 performs short-distance wireless communication with the external unit 100. In this embodiment, the information processor 101 is a wristwatch type of information processor, so that it is usually worn by the owner (user) on his or her wrist at all times, and therefore it enables the possessor (user) to recognize whether or not a distance between the possessor (user) and the external unit 100 is within such a range that short-distance communication is possible".

I. "[0025] The transmission section 305 may use a high-security digital communication system, e.g., a spread-spectrum system or the like. Also, data themselves may be encrypted. The function of the transmission section 305 can be realized by the I/F 205 shown in FIG. 2. The attachment/detachment detection section 308 detects detachment of the wristwatch type information processor 101 from the wrist. Specifically, the function of the attachment/detachment detection section 308 is realized by the attachment/detachment sensor 204. The attachment/detachment sensor 204 may be, for example, any of a temperature sensor (for sensing, for example, body heat to detect a change in temperature at the time of attachment or detachment), a pressure sensor (for sensing, for example, a pressure relating to closeness of contact with the

wrist to detect pressure based on closeness of contact at the time of attachment or detachment), a pulse sensor (for sensing, for example, the existence/nonexistence of a pulse at the time of attachment or detachment), and an optical sensor (for sensing, for example, light shielded at the time of wearing).

[0026] When detachment of the wristwatch type information processor 101 from the wrist is detected with the attachment/detachment sensor 204, information on the occurrence of detachment is transmitted from the transmission section 307 to the external unit 100 to make a below-described authentication procedure invalid, thereby ensuring security of the external unit 101 even if the wristwatch type information processor 101 is stolen, for example. Further, the external unit 100 includes a receiving section 309, an updated information storage section 310, and an authentication section 311. The receiving section 309 receives the latest items in authentication data and collation date information transmitted from the information processor 101, and decodes the received data. The function of the receiving section 309, although unillustrated, can be realized by the same hardware as the I/F 205 shown in FIG. 2".

No. 5. The invention described in Cited Document 1

1. According to the description in A above, "The versatile device is implemented as a wristwatch. The wristwatch is configured to facilitate a wireless transaction for an authenticated user and is configured to be worn by the authenticated user so as to encircle a part of the authenticated user," the description in B above, "The wristwatch 100 includes an electronic circuitry 50 to host one or more applications, secure authentication/identification data, and transaction data, and to validate use and possession of the wristwatch 100 by a legitimate user by executing a use-based context security validation scheme," the description in D above, "a user wears the wristwatch 100. Moreover, in Step 320, the user goes through a security initialization procedure to authenticate the user prior to allowing the user general operational use of application hosting functionality of the wristwatch 100 to facilitate a variety of wireless transactions for the authenticated user. The initialization procedure may be a simple wristwatch-based operation (e.g. entering a PIN number on the wristwatch itself) or a more complex security procedure involving an external security system in Step 325 (e.g. an external device with retina scanning hardware could be used to provide unique user verification, which is conveyed to the wristwatch 100 via the encrypted RF data communications link 302). Whatever the chosen initialization method, its task is to activate authenticated use of the wristwatch 100 by validating both the user and the data channel 80 integrated into the straps of the wristwatch 100," and also the description in D above,

"Once the user is authenticated, the wristwatch 100 enters an active/secure status state (in Step 330) and starts execution of one or more applications, which are configured to facilitate wireless transactions and services," in Cited Document 1,
it can be read that "a versatile device implemented as a wristwatch is equipped with an electronic circuitry to host secure authentication authenticating a user, and once the user is authenticated, the wristwatch enters an active/secure status".

2. According to the description in A above, "the integration of a data channel within the straps of the wristwatch itself enables validation of whether or not the wristwatch is being worn by the authenticated user that initiated use of the wristwatch. Removal of the wristwatch will invalidate its context security and place the wristwatch in an inactive state," the description in B above, "the wristwatch 100 includes a validation mechanism for controlling use of the wristwatch 100 based on whether or not the authenticated user continues to wear the wristwatch 100 after initiating use of the wristwatch 100. The validation mechanism includes a transmitting element 40, a receiving element 30, a data channel 80, and a monitoring component (integrated in the electronic circuitry 50) for monitoring the status of the data channel 80," also the description in B above, "a data channel 80 enabling validation of whether or not the wristwatch 100 is being worn by the authenticated user that initiated use of the wristwatch 100. Removal of the wristwatch 100 will invalidate its context security and place the wristwatch in an inactive state, disabling all external interaction via the wireless link," the description in C above, "the wristwatch 100 integrates a data channel 80 within the first and second straps 10 and 20 of the wristwatch 100 itself enabling validation of whether or not the wristwatch 100 is being worn by the authenticated user that initiated use of the wristwatch 100. The wristwatch body 90 includes an embedded electronics subsystem 50, a transmitting element 40 for transmitting data through the data channel 80, a receiving element 30 for receiving the data transmitted through the data channel 80, and optional biosensors 70 for sensing whether or not the authenticated user is wearing the wristwatch 100. A successful transmission of the data between the transmitting element 40 and the receiving element 30 indicates that the wristwatch 100 is being worn by the authenticated user. Moreover, the data channel 80 is configured to be rendered inoperable if the authenticated user discontinues wearing the wristwatch 100," the description in D above, "Security can be enhanced by using the optional biosensor subsystem 70 and 71, providing the capability to detect the presence or absence of the authenticated user's body using biometric measurement techniques (e.g., skin temperature, light reflection, humidity), in addition to the integrity

of the data channel 80 itself," also the description in D above, "If a change in the active/secure status state is detected because the data channel has become inoperable indicating the authenticated user has removed the wristwatch 100, the wristwatch 100 erases (in Step 360) its active/secure status state and application data and then switches (in Step 365) to an inactive state or off," and also the description in D above, "The optional bio-sensing subsystem (in Step 340) provides an extra level of security by determining the user's presence as a supplement to the monitoring of the status and integrity of the data channel 80," in Cited Document 1,
it can be said that "a wristwatch body includes a data channel enabling validation of whether or not a wristwatch is being worn by an authenticated user that initiated use of the wristwatch, and a biosensor providing a capability to detect the presence or absence of the authenticated user's body, and removal of the wristwatch will invalidate its context security and place the wristwatch in an inactive state, disabling all external interaction via a wireless link".

3. According to the description in B above, "the wristwatch 100 will be allowed to accept or deny any external service interaction via a wireless link, based on whether the wristwatch 100 is in an active/secure status state or in an inactive state," the described contents in D above which were cited in 1. above, also the description in D above, "when the wristwatch 100 is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch 100, the particular application checks in Step 380 whether or not the wristwatch 100 is operating in the active/secure status state," also the description in D above, "If it is operating, the particular application then checks in Step 385, the validity of the interrogation," and also the description in D above, "If it is valid, in Step 395, the particular application executes the desired service or transaction supported by the particular application," in Cited Document 1,
it can be read that "once the user is authenticated, a wristwatch enters an active/secure status state, and in the active/secure status state, when the wristwatch is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch, the validity of the interrogation is checked, and if the interrogation is valid, the particular application executes the wireless transaction supported by the particular application".

4. As described above, from the matters examined in 1. to 3. above, it is recognized that Cited Document 1 described the following invention (hereinafter, referred to as the

"Cited Invention").

"A versatile device implemented as a wristwatch comprising an electronic circuitry to host secure authentication authenticating a user, once the user is authenticated, the wristwatch entering an active/secure status,

wherein a wristwatch body includes a data channel enabling validation of whether or not the wristwatch is being worn by an authenticated user that initiated use of the wristwatch;

and a biosensor providing a capability to detect the presence or absence of the authenticated user's body,

wherein removal of the wristwatch will invalidate its context security and place the wristwatch in an inactive state, disabling all external interaction via a wireless link, and

wherein in the active/secure status state, when the wristwatch is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch, the validity of the interrogation is checked, and if the interrogation is valid, the particular application executes the wireless transaction supported by the particular application".

No. 6. Comparison of the Invention and the Cited Invention

1. Since a "versatile device implemented as a wristwatch" in the Cited Inventions executes a "transaction" when a state in which a "user" is "authenticated" is kept,

it corresponds to a "trusted device" in the Invention.

2. Since in the Cited Invention, a "user" is "authenticated" with a "wristwatch" being worn, and if the "user" is "authenticated," it enters an "active/secure status state,"

the matter that the "wristwatch" in the Cited Invention enters the "active/secure status state" corresponds to

"switching the trusted device to an authenticated state" of the Invention,

so that "once the user is authenticated, the wristwatch entering an active/secure status" in the Cited Invention corresponds to

"thereby switch said trusted device to an authenticated state" in the Invention.

Since in the Cited Invention, an "electronic circuitry" of the "wristwatch" is "to host secure authentication authenticating a user," and thereby the "wristwatch" transitions to the "active/secure status state,"

the "electronic circuitry" in the Cited Invention corresponds to

"authentication circuitry" in the Invention.

The fact pointed out above that "a 'user' is 'authenticated' with a 'wristwatch' being worn" is nothing more than "a user physically possessing the trusted device,"

so that "a versatile device implemented as a wristwatch comprising an electronic circuitry to host secure authentication authenticating a user, once the user is authenticated, the wristwatch entering an active/secure status" in the Cited Invention corresponds to

" authentication circuitry configured to authenticate with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state" in the Invention.

3. In the Cited Invention, a "data channel" is one "enabling validation of whether or not the wristwatch is being worn by an authenticated user that initiated use of the wristwatch," and

"validation of whether or not the wristwatch is being worn by an authenticated user that initiated use of the wristwatch" in the Cited Invention corresponds to

"to monitor physical possession of the trusted device by the user in accordance with the authentication operation" in the Invention, and

"removal of the wristwatch will invalidate its context security and place the wristwatch in an inactive state" in the Cited Invention corresponds to

"to switch the trusted device from the authenticated state if the trusted device is no longer physically owned by the user" in the Invention.

Since a "data channel" in the Cited Invention "validates" that "the wristwatch is not being worn by an authenticated user that initiated use of the wristwatch" to detect that the "user" "removes the wristwatch," thereby "invalidating security and placing the wristwatch in an inactive state,"

the "data channel" in the Cited Invention includes an embodiment "placing the wristwatch in an inactive state, if detecting that the authenticated user that initiated use of the wristwatch removes the wristwatch".

Therefore,

"a data channel placing the wristwatch in an inactive state if detecting the authenticated user that initiated use of the wristwatch removes the wristwatch" in the Cited Invention which was examined above corresponds to

" retention monitoring circuitry configured to monitor physical possession of said trusted device by said user following said authentication operation and to switch said trusted device out of said authenticated state if said trusted device is not in physical

possession of said user" in the Invention.

4. An "external device" in Cited Invention and
(1) a "target device that is one of a plurality of different target devices" in the Invention are common in the point that each of them is "an external device," and

"the wristwatch is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch" in the Cited Invention, and

"a request to establish communication received from a target device that is one of a plurality of different target devices" in the Invention
are common in the point that each of them "requests to establish communication received from an external device".
(2) Since in the Cited Invention, "when interrogated, the validity of the interrogation is checked," in the Cited Invention, it is obvious that any configuration in which a "wristwatch" "detects" that the "interrogation" has been received is encompassed, so that it is obvious that any configuration in the "wristwatch" is "detection means" for "detecting" the "interrogation" also in the Cited Invention.

Therefore, the "detection means" in which "when the wristwatch is interrogated by an external device to request information or to initiate a wireless transaction supported by a particular application hosted by the wristwatch, the validity of the interrogation is checked" in the Cited Invention, and

" communication triggering circuitry configured to detect a request to establish communication received from a target device that is one of a plurality of different target devices" in the Invention
are common in the point that each of them is " communication triggering circuitry configured to detect a request to establish communication received from an external device".
(3) In the Cited Invention, "if the interrogation is valid, the particular application executes the wireless transaction supported by the particular application," is nothing but performing "communication" with an "external device," and therefore, it is obvious that a "wristwatch" has a "communication circuit" to "communicate" with an "external device".

Then, the "communication with an external device" is performed "in the active/secure status state," and

since the "active/secure status state" in the Cited Invention corresponds to

"said trusted device is in said authenticated state" in the Invention,

"if the interrogation is valid, the particular application executes the wireless transaction supported by the particular application" in the Cited Invention, and

" communication circuitry configured to communicate with said target devices if said trusted device is in said authenticated state" in the Invention

are common in the point that each of them is communication circuitry configured to communicate with the external device if said trusted device is in the authenticated state.

5. From the matters examined in 1. to 4. above, corresponding features and different features of the Invention and the Cited Invention are as follows.

[Corresponding Feature]

"A trusted device comprising:

authentication circuitry configured to authenticate with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring circuitry configured to monitor physical possession of said trusted device by said user following said authentication operation and to switch said trusted device out of said authenticated state if said trusted device is not in physical possession of said user,

communication triggering circuitry configured to detect a request to establish communication received from an external device; and

communication circuitry configured to communicate with said external device if said trusted device is in the authenticated state.

[Different Feature 1]

Regarding "retention monitoring circuitry,"

in the Invention, it is "said retention monitoring circuitry being equipped with one or more detection circuits including a photo-detector shielded from light when said trusted device is physical possession of said user,"

whereas, in the Cited Invention, there is no mention about "being equipped with one or more detection circuits including a photo-detector shielded from light when said trusted device is physical possession of said user".

[Different Feature 2]

Regarding "an external device,"

in the Invention, it is "a target device that is one of a plurality of different target devices",

whereas, in the Cited Invention, it is "an external device".

No. 7 Judgment by the body regarding the different features

1. Regarding [Different Feature 1]

As described in the Well-known literature cited in H and I above, it was a well-known technical matter for a person skilled in the art before the filing of the present application in the first country that "an optical sensor for sensing light shielded at the time of wearing is used for detecting the attachment/detachment of the wristwatch type information processor" (see the underlined descriptions and the like of H and I above), and the Cited Invention and a "wristwatch type information processor" described in the Well-known literature have generally the same configuration. Even in the Cited Invention, as mentioned in the description cited in E above, although a method is different, "light" is used for detecting the attachment/detachment of a "wristwatch" of a "user,"

so that in the Cited Invention, it is a matter which can be appropriately achieved by a person skilled in the art to configure to detect the attachment/detachment of the "wristwatch" using the "optical sensor" described in the Well-known literature, instead of the description cited in E above.

Accordingly, [Different Feature 1] is not exceptional.

2. Regarding [Different Feature 2]

In Cited Document 2 cited in F and G above,
it is described to "perform wireless communication with any of a plurality of different wireless transaction devices (corresponding to "target devices" in the Invention) in a wristwatch type device (corresponding to "a trusted device" in the Invention) that is activated by being worn by a correct user authenticated using biometric data," and it had been a well-known technical matter for a person skilled in the art to "receive from a target device that is one of a plurality of different target devices" (see, the underlined descriptions and the like of F and G above) before the filing of the present application in the first country.

The technical matters described in the Cited Invention and Cited Document 2 are common in the point that each of them is "a device that can be used when being worn by an authorized user after authentication, performing wireless communication with an external device," and there is no particular restriction on the "external device" in the Cited Invention, so that it is a matter which can be appropriately achieved by a person skilled in the art that as the "external device" in the Cited Invention, it is configured to

"establish communication received from one of a plurality of different external devices".

Accordingly, [Different Feature 2] is not exceptional.

3. As examined in 1. and 2. above, neither [Different Feature 1] nor [Different Feature 2] is exceptional, and effects achieved by the configuration of the Invention could be easily predicted by a person skilled in the art, and cannot be regarded as an exceptional feature.

No. 8. Regarding Article 36(6)(ii)

Although Claim 3 of claims amended by the written amendment dated April 22, 2019 (hereinafter, referred to as "the claim of the present application) describes ". . . includes the creation of credentials usable in an authentication process," it is still unclear how to realize the "creation of credentials" even if examining Claim 3 of the present application and the contents described in other claims.

No. 9. Closing

Therefore, the Invention could have been easily made by a person skilled in the art according to the Cited invention, the technical matters described in Cited Document 2, and the technical matters described in the Well-known literature, and thus the Appellant should not be granted a patent for it under the provisions of Article 29(2) of the Patent Act.

In addition, the present application does not satisfy the requirement of Article 36(6)(ii) of the Patent Act.

Therefore, the appeal decision shall be made as described in the conclusion.

April 22, 2020

Chief administrative judge: TANAKA, Hideto
Administrative judge: ISHII, Shigekazu
Administrative judge: YAMAZAKI, Shinichi