# PATROLL Winning Submission

## U.S. Patent 10,083,285

U.S. Patent 10,083,285 ("*Factor 2*" or the "patent-at-issue") was filed on December 6, 2017, and claims an earliest priority date on August 29, 2001. Claim 1 of the patent-at-issue describes a method of an enhanced authentication process for users accessing an online system through a computer network. Initially, the online system receives user-authentication information, which includes a user-authentication code generated by an authentication system. This code is provided to the user after an attempt to access the online system and is designed to be valid for a specific period. Importantly, the code becomes invalid either after its predetermined time expires or after its first use. The online system then sends a user-authentication request to the authentication system, incorporating both the user-authentication code and user-identification information. The online system then awaits a response from the authentication system, which confirms or denies the user's authentication based on the validity of the provided code. If authenticated, the online system grants the user access to the requested information.

The primary reference, U.S. Patent 7,287,270 ("*Arkray*"), was filed on October 30, 2001, and claims an earliest priority date October 31, 2000. The patent describes a method involving a service provider's server device authenticating a user on a network. When a user sends a network connection request to an Internet server, the server replies with an authentication confirmation number generated by a random number generator. The user then connects their portable telephone to a modem and inputs the received authentication number using the telephone's keypad. An authentication unit verifies the connection request by checking if the telephone number stored in the user information storage matches the one received by the modem and if the entered authentication number is correct. If both conditions are met, the authentication unit allows the connection to the network to proceed.

The primary reference, U.S. Patent 7,765,580 ("*Entrust*"), was filed on May 14, 2001, and claims an earliest priority date on December 22, 2000. The patent describes a method of authenticating a user by initially sending primary authentication information, like user identification or password data, to an authentication unit over the Internet. This unit generates a session-based authentication code and sends it to a destination unit through a first secondary channel. The destination unit subsequently forwards this code to the first unit via a second secondary channel in a manner that remains unnoticed by the user of the first unit. The first unit then sends the received authentication code back to the authentication unit over the primary channel within the same session. Finally, the authentication unit authenticates the user if the returned authentication code is deemed valid.

The secondary reference, U.S. Pat. App. 2002/0007462 ("*Mitsubishi*"), was filed on June 5, 2001, and claims an earliest priority date on July 11, 2000. The patent application describes a user authentication system which includes a communication terminal device with voice input capabilities, allowing users to log into a system requiring successful authentication via unique user identification information and corresponding passwords. A user authentication database stores both user identification and voiceprint information, with voiceprints obtained when users speak their identification details. The system features a one-time identification information management component that generates a unique code upon receiving code-format identification from the communication terminal. This code is sent back to the terminal and recorded in the database as a temporary password. Upon successful authentication, the temporary password status is updated. The communication terminal includes a code-format identification transmitter, a voice-format identification transmitter, and an automatic login feature that uses the generated one-time identification after successful authentication.

A sample claim chart comparing claim 1 of *Factor 2* to *Arkray*, *Entrust*, and *Mitsubishi* is provided below.

| **US10083285** (“*Factor 2*”) | **A. US7287270** (*“Arkray”*)<br>**B. US7765580** (*“Entrust”*)<br>**C. US20020007462** (*“Mitsubishi”*) |
|---|---|
| 1.pre. A method of enhancing **authentication of a user attempting to access an online system via a computer network**, the method comprising: | **A. US7287270**<br>“1. A method for **authenticating a user by which a server device of a service provider authenticates a service user on a network**, the method comprising: . . . .” *Arkray* at claim 1<br><br>**B. US7765580**<br>“Briefly, a method and apparatus provides **user authentication by communicating primary authentication information, such as user identification data and/or password data to an authentication unit via a primary channel such as over the Internet**.” *Entrust* at col. 3:15-19<br><br>**C. US20020007462**<br>“1. A **user authentication system which, to permit a log-in from a communication terminal device** with a voice input-function, **conducts user authentication based on user identification information uniquely identifying each user** and a password corresponding to the user identification information, said system comprising: . . . .” *Mitsubishi* at claim 1<br><br>“FIG. 1 is a system configuration diagram illustrating one embodiment of the **user authentication system** according to the present invention. A **user of a cellular phone** 1 **with an Internet function can converse with a party connected online** via a packet communication network of the cellular phone manufacturer, **and can also connect to the Internet** and use various services offered by a service provider.” *Mitsubishi* at par. 0023 |
| 1.a. **receiving** by the online system, via the computer network, **user-authentication information including a user-authentication code provided by an authentication system to the user via the computer network after an attempt by the user to access information of the online system**, wherein: | **A. US7287270**<br>“The **user accesses the server** 1 of the office from the personal computer 2 **via the Internet** 5.” *Arkray* at col. 5:59-60<br><br>“1. A method for authenticating a user by which a server device of a service provider authenticates a service user on a network, the method comprising: |

| | |
|---|---|
| *(cont.)*<br>1.a. **receiving** by the online system, via the computer network, **user-authentication information including a user-authentication code provided by an authentication system to the user via the computer network after an attempt by the user to access information of the online system**, wherein: | a confirmation information issuing step including **receiving an authentication request from a first communication device of the service user, and then generating a confirmation information to be replied to the first communication device**; . . . ." *Arkray* at claim 1<br><br>**B. US7765580**<br>"An **authentication code is first generated by the authentication unit on a per session basis** and is sent to the first device via an alternate or secondary channel during the session." *Entrust* at col. 3:19-22<br><br>"Referring also to FIG. 2, the operation of the system shown in FIG. 1 will be explained. During a registration process, **a user registers with the authentication unit**. The **authentication unit creates a database entry for each user (or user device) that contains a user ID field, a password verification field (if used, or a one-way hash of the password) and a device address field**. As shown in block 200, a method for **providing user authentication includes sending**, by the first unit 10, **user identification data, such as the user ID** on the primary channel 14 to the second device 12 which also serves, in this embodiment, as an authentication unit." *Entrust* at col. 4:56-66<br><br>**C. US20020007462**<br>"1. A **user authentication system which, to permit a log-in from a communication terminal device** with a voice input-function, **conducts user authentication based on user identification information uniquely identifying each user and a password corresponding to the user identification information**, said system comprising: . . . ." *Mitsubishi* at claim 1<br><br>"**When accessing the Internet, a channel connection is established via a data communication network** 3 **with a log-in site** specified by designating an address." *Mitsubishi* at par. 0023<br><br>"In the user authentication database 9, **a company member ID and a voiceprint information obtained when the company member ID is pronounced by the corresponding company member are stored in correlation to one another. The company member ID of the present embodiment corresponds to the user identification information registered in the company proprietary system for identifying a user**." *Mitsubishi* at par. 0025 |

| | |
|---|---|
| 1.b. the **user-authentication code is information generated by the authentication system** for authenticating the user, | **A. US7287270**<br>"If it can be confirmed that the sent user number and password agree with the user number and password registered in advance, **the authentication unit** 16 **allows a random number generating unit** 13 **(confirmation information generating unit) to generate random numbers and the random numbers are sent as a confirmation number (confirmation information) to the user's personal computer** 2 (step S3). For example, the random numbers generated by the random generating unit 13 is, for example, "4756," and the confirmation number "4756" is sent to the user's personal computer 2." *Arkray* at col. 6:30-40<br>**B. US7765580**<br>"An **authentication code is first generated by the authentication unit on a per session basis** and is sent to the first device via an alternate or secondary channel during the session." *Entrust* at col. 3:19-22<br>**C. US20020007462**<br>"The **onetime ID managing section** 10 **generates a onetime ID upon receiving a code-format company member ID from the cellular phone** 1 **via the data communication network**. The onetime ID managing section 10 then transmits the generated onetime ID back to the cellular phone 1 via the data communication network 3, and also records, in the user authentication database 9 in correlation with the company member ID concerned, a disallowed state of the log-in designating the onetime ID as the password." *Mitsubishi* at par. 0026 |
| 1.c. the **user-authentication code is configured to be valid for a predetermined time**, | **B. US7765580**<br>"An **authentication code is first generated by the authentication unit on a per session basis** and is sent to the first device via an alternate or secondary channel during the session." *Entrust* at col. 3:19-22<br>"The **authentication controller** 502 **may include a time out period during which time a reset condition will occur to request an authentication code again via the primary channel if the authentication code is not received via the second secondary channel within a fixed period of time**." *Entrust* at col. 11:23-28 |

| | |
|---|---|
| *(cont.)*<br>1.c. the **user-authentication code is configured to be valid for a predetermined time**, | **C. US20020007462**<br>“As described below in further detail, **a onetime ID, which is generated and deleted during an authentication process, is stored in correlation with the company member ID**. **A onetime ID is a password that can be used only once**.” *Mitsubishi* at par. 0025<br>“The onetime ID managing section 10 generates a onetime ID upon receiving a code-format company member ID from the cellular phone 1 via the data communication network. **The onetime ID managing section** 10 **then transmits the generated onetime ID back to the cellular phone** 1 **via the data communication network** 3**, and also records, in the user authentication database** 9 **in correlation with the company member ID concerned, a disallowed state of the log-in designating the onetime ID as the password**.” *Mitsubishi* at par. 0026 |
| 1.d. the **user-authentication code is configured to become invalid after the predetermined time**, and | **B. US7765580**<br>“An **authentication code is first generated by the authentication unit on a per session basis** and is sent to the first device via an alternate or secondary channel during the session.” *Entrust* at col. 3:19-22<br>“The **authentication controller** 502 **may include a time out period during which time a reset condition will occur to request an authentication code again via the primary channel if the authentication code is not received via the second secondary channel within a fixed period of time**.” *Entrust* at col. 11:23-28<br>**C. US20020007462**<br>“As described below in further detail, **a onetime ID, which is generated and deleted during an authentication process, is stored in correlation with the company member ID**. **A onetime ID is a password that can be used only once**.” *Mitsubishi* at par. 0025<br>“**Upon confirmation of the user log-in, the web server** 4 **immediately and automatically deletes the onetime ID corresponding to that user using the onetime ID deleting section** 12 (step 111). In this way, **unauthorized log-in through re-use of the onetime ID is prevented**. Subsequently, a main screen of the company system as shown for example in FIG. 4(c) is displayed on the cellular phone 1 |

| | |
|---|---|
| | (step 112). Because multiple log-ins by a single user are prohibited in the company proprietary system of the present embodiment, a log-in using the company member ID remains disallowed at this point." *Mitsubishi* at par. 0037 |
| 1.e. the **user-authentication code is configured to become invalid after a first use** to authenticate the user; | **B. US7765580**<br>"An **authentication code is first generated by the authentication unit on a per session basis** and is sent to the first device via an alternate or secondary channel during the session." *Entrust* at col. 3:19-22<br>**C. US20020007462**<br>"**Upon confirmation of the user log-in, the web server** 4 **immediately and automatically deletes the onetime ID corresponding to that user using the onetime ID deleting section** 12 (step 111). In this way, **unauthorized log-in through re-use of the onetime ID is prevented**. Subsequently, a main screen of the company system as shown for example in FIG. 4(c) is displayed on the cellular phone 1 (step 112). Because multiple log-ins by a single user are prohibited in the company proprietary system of the present embodiment, a log-in using the company member ID remains disallowed at this point." *Mitsubishi* at par. 0037 |
| 1.f. **providing by the online system**, via the computer network, **a user-authentication request to the authentication system**, wherein **the user-authentication request includes the user-authentication code and user-identification information of the user**; | **A. US7287270**<br>"If it can be confirmed that the sent user number and password agree with the user number and password registered in advance, the authentication unit 16 allows a random number generating unit 13 (confirmation information generating unit) to generate random numbers and the random numbers are sent as a confirmation number (confirmation information) to the user's personal computer 2 (step S3). For example, **the random numbers generated by the random generating unit** 13 **is, for example, "4756," and the confirmation number "4756" is sent to the user's personal computer** 2." *Arkray* at col. 6:30-40<br>"**When the confirmation number receiving unit** 15 **receives the confirmation number "4756" from the portable number** 3, **it sends the received confirmation number and the telephone number "090xxxxyyyy" of the portable telephone** 3 obtained in the step S5 **to the authentication unit** 16 **as the user information**. Then, the authentication unit 16 compares the user information sent from the confirmation number receiving unit 15 with the confirmation number issuing |

| | |
|---|---|
| *(cont.)*<br>1.f. **providing by the online system**, via the computer network, **a user-authentication request to the authentication system**, wherein **the user-authentication request includes the user-authentication code and user-identification information of the user**; | information stored in the confirmation number storage unit 14 (step S7).” *Arkray* at col. 7:20-29<br><br>**B. US7765580**<br>“This is done by searching the authentication database 18 as indexed by the received user ID from the primary authentication information sent by the first unit 10. The second unit 12 **matches the received user ID and if a password is used the associated hashed password, that was previously stored during the registration process** to determine the appropriate destination unit identifier. The **received password may be hashed and compared to the stored hash password**. If there is a correlation, then the primary authentication is said to have succeeded, and the secondary authentication process may proceed using the destination unit identifier.” *Entrust* at col. 5:12-18<br><br>**C. US20020007462**<br>“1. A user authentication system which, to permit a log-in from a communication terminal device with a voice input-function, **conducts user authentication based on user identification information uniquely identifying each user and a password corresponding to the user identification information**, said system comprising: . . . .” *Mitsubishi* at claim 1<br><br>“2. A user authentication system comprising:<br>. . .<br>a onetime identification information managing means which generates **a onetime identification information upon receipt of a code-format user identification information from said communication terminal device via a data communication network**, **transmits said generated onetime identification information back to said communication terminal device via said data communication network**, and records, in said user authentication database in correlation with said user identification information, **a disallowed state of a log-in designating said onetime identification information as the password**; and . . . . ” *Mitsubishi* at claim 2 |
| 1.g. **receiving by the online system**, via the computer network, **a response to the user-authentication request indicating whether the authentication system authenticated the user**, wherein: | **A. US7287270**<br>“6. An authentication device comprising:<br>. . .<br>**an authentication unit for juduing [sic] whether or not the confirmation information received by the confirmation information receiving unit agrees with the confirmation** |

| | |
|---|---|
| *(cont.)*<br>1.g. **receiving by the online system**, via the computer network, **a response to the user-authentication request indicating whether the authentication system authenticated the user**, wherein: | **information stored in the confirmation information storing unit**, . . . .” *Arkray* at claim 6<br><br>**B. US7765580**<br>“This is done by searching the authentication database 18 as indexed by the received user ID from the primary authentication information sent by the first unit 10. The second unit 12 **matches the received user ID and if a password is used the associated hashed password, that was previously stored during the registration process** to determine the appropriate destination unit identifier. The **received password may be hashed and compared to the stored hash password**. **If there is a correlation, then the primary authentication is said to have succeeded, and the secondary authentication process may proceed** using the destination unit identifier.” *Entrust* at col. 5:12-18<br><br>“As shown in block 204, the method includes **sending the authentication code generated by the authentication code generator** 28, **such as a random number, or a derivation of the authentication code, during the same session to the determined destination unit that was determined based on the user ID** and the destination address 22.” *Entrust* at col. 5:33-38<br><br>**C. US20020007462**<br>“2. A user authentication system comprising:<br>. . .<br>**a user authenticating means** which, upon receipt of voice-format user identification information from said communication terminal device via a telephone network, conducts voiceprint authentication using said voice-format user identification information by referring to said user authentication database, and, **when the authentication is successful, changes to an allowed state said state recorded in said user authentication database concerning the log-in by said onetime identification information**; wherein<br>. . .<br>**an automatic log-in means for, after the authentication is completed by said user authenticating means, automatically logging into said system using said onetime identification information received from said onetime identification information managing means**.” *Mitsubishi* at claim 2 |

| | |
|---|---|
| 1.h. the **user is authenticated using the user-authentication code and the user-identification information included in the authentication request**, | **A. US7287270**<br>“When **the authentication unit** 16 **confirms that the user information (telephone number “090xxxxyyyy” and confirmation number “4756”) obtained from the confirmation number receiving unit** 15 **agrees with the telephone number and the confirmation number** stored in the confirmation number storage unit 14, respectively, **it authenticates that the connection request via the user number (ARK00750) and the password (ADLN01) is sent from the user in person and authorizes the connection** from the personal computer 2 to the server 1 (step S8). Thereafter, the user can use resources on the LAN in an office via the server 1.” *Arkray* at col. 7:30-40<br><br>**B. US7765580**<br>“For example, the second unit 12 may **store the generated authentication code from the authentication code generator** 28 **during the session and compare the resent authentication code** 36 **to the stored authentication code**. **If they match, the user is authenticated**. As shown in block 210, the method includes waiting for a next session to authenticate the same or another user.” *Entrust* at col. 5:56-62<br><br>**C. US20020007462**<br>“2. A user authentication system comprising:<br>. . .<br>**an automatic log-in means for, after the authentication is completed by said user authenticating means, automatically logging into said system using said onetime identification information received from said onetime identification information managing means**.” *Mitsubishi* at claim 2 |
| 1.i. the **response to the user-authentication request confirms authentication of the user if the user-authentication code is valid**, and | **A. US7287270**<br>“When **the authentication unit** 16 **confirms that the user information (telephone number “090xxxxyyyy” and confirmation number “4756”) obtained from the confirmation number receiving unit** 15 **agrees with the telephone number and the confirmation number** stored in the confirmation number storage unit 14, respectively, **it authenticates that the connection request via the user number (ARK00750) and the password (ADLN01) is sent from the user in person and authorizes the connection** from the personal computer 2 to the server 1 (step S8). Thereafter, |

| | |
|---|---|
| *(cont.)*<br>1.i. the **response to the user-authentication request confirms authentication of the user if the user-authentication code is valid**, and | the user can use resources on the LAN in an office via the server 1." *Arkray* at col. 7:30-40<br>**B. US7765580**<br>"1. A method for providing user authentication comprising:<br>. . .<br>(f) **authenticating the user when the returned authentication code is determined to be suitable**." *Entrust* at claim 1<br>**C. US20020007462**<br>"**When authentication is successful, the user authenticating section** 11 **resets the state concerning the log-in by the onetime ID recorded in the user authentication database** 9 **to an allowed state**. Upon completion of the user log-in from the cellular phone 1, the onetime ID deleting section automatically deletes the corresponding onetime ID from the user authentication database 9." *Mitsubishi* at par. 0026 |
| 1.j. the **response to the user-authentication request denies authentication of the user if the user-authentication code is invalid**; and | **A. US7287270**<br>"Furthermore, according to this embodiment, as the second authentication requester information, **the user's telephone number is used and this telephone number is obtained from a calling telephone number notification service, making it difficult for the third person to pretend to be the user in person**. Thus, it is possible to prevent the wrongdoing reliably." *Arkray* at col. 8:8-14<br>"4. The method for authenticating a user according to claim 1: the method further comprising, in the authentication step **after it is judged that the confirmation information replied to the first communication device agrees with the confirmation information sent from the service user by the second communication device**, a step of receiving credit card information of the service user from the second communication device and charging the service user based on the received credit card information." *Arkray* at claim 4<br>**C. US20020007462**<br>"When the user confirms the completion of authentication through the audio guidance provided by the CTI server 6, the user presses the OK button according to the guidance displayed on the authentication screen (step 108). In response, the automatic log-in unit 17 transmits the internally retained onetime ID to the web server 4 so as to automatically log into |

| | |
|---|---|
| *(cont.)*<br>1.j. the **response to the user-authentication request denies authentication of the user if the user-authentication code is invalid**; and | the system. **The log-in is possible at this point because the state of log-in by the onetime ID is changed to the allowed state** in the step 206 **after proper authentication of the user**. If the OK button is pressed before the user is authenticated, **log-in is unsuccessful because the state of log-in by the onetime ID remains disallowed until authentication has been successfully performed**.” *Mitsubishi* at par. 0036 |
| 1.k. **providing by the online system**, via the computer network, **the user access to the information of the online system**. | **A. US7287270**<br>“When **the authentication unit** 16 **confirms that the user information (telephone number “090xxxxyyyy” and confirmation number “4756”) obtained from the confirmation number receiving unit** 15 **agrees with the telephone number and the confirmation number** stored in the confirmation number storage unit 14, respectively, **it authenticates that the connection request via the user number (ARK00750) and the password (ADLN01) is sent from the user in person and authorizes the connection from the personal computer** 2 **to the server** 1 (step S8). Thereafter, **the user can use resources on the LAN in an office via the server** 1.” *Arkray* at col. 7:30-40<br>**B. US7765580**<br>“For example, the second unit 12 may **store the generated authentication code from the authentication code generator** 28 **during the session and compare the resent authentication code** 36 **to the stored authentication code**. **If they match, the user is authenticated**. As shown in block 210, the method includes waiting for a next session to authenticate the same or another user.” *Entrust* at col. 5:56-62<br>“The second unit 302 passes the resent authentication code to the authentication unit 304 where **the authentication unit** 304 **compares the resent authentication code with the authentication code** that was sent to the third unit 306. **If they match, the user** (i.e. first unit) **is granted access**.” *Entrust* at col. 7:29-34<br>**C. US20020007462**<br>“2. A user authentication system comprising:<br>. . .<br>**an automatic log-in means for, after the authentication is completed by said user authenticating means, automatically logging into said system using said onetime identification information received from said onetime** |

| | |
|---|---|
| *(cont.)*<br>1.k. **providing by the online system**, via the computer network, **the user access to the information of the online system**. | **identification information managing means**." *Mitsubishi* at claim 2 |