

Oral Argument

Unified Patents and JPMorgan Chase Bank v. Dynapass IP Holdings, LLC (Patent Owner)

IPR2023-00425
U.S. Patent No. 6,993,658
April 16, 2024

Unpatentability Grounds

Ground	References	Challenged Claims
1	<i>Veneklase</i> in view of <i>Jonsson</i>	5
2	<i>Kew</i> in view of <i>Sormunen</i>	1, 3-6

Pet., p. 2.

'658 Patent: "Use of personal communication devices for user authentication"

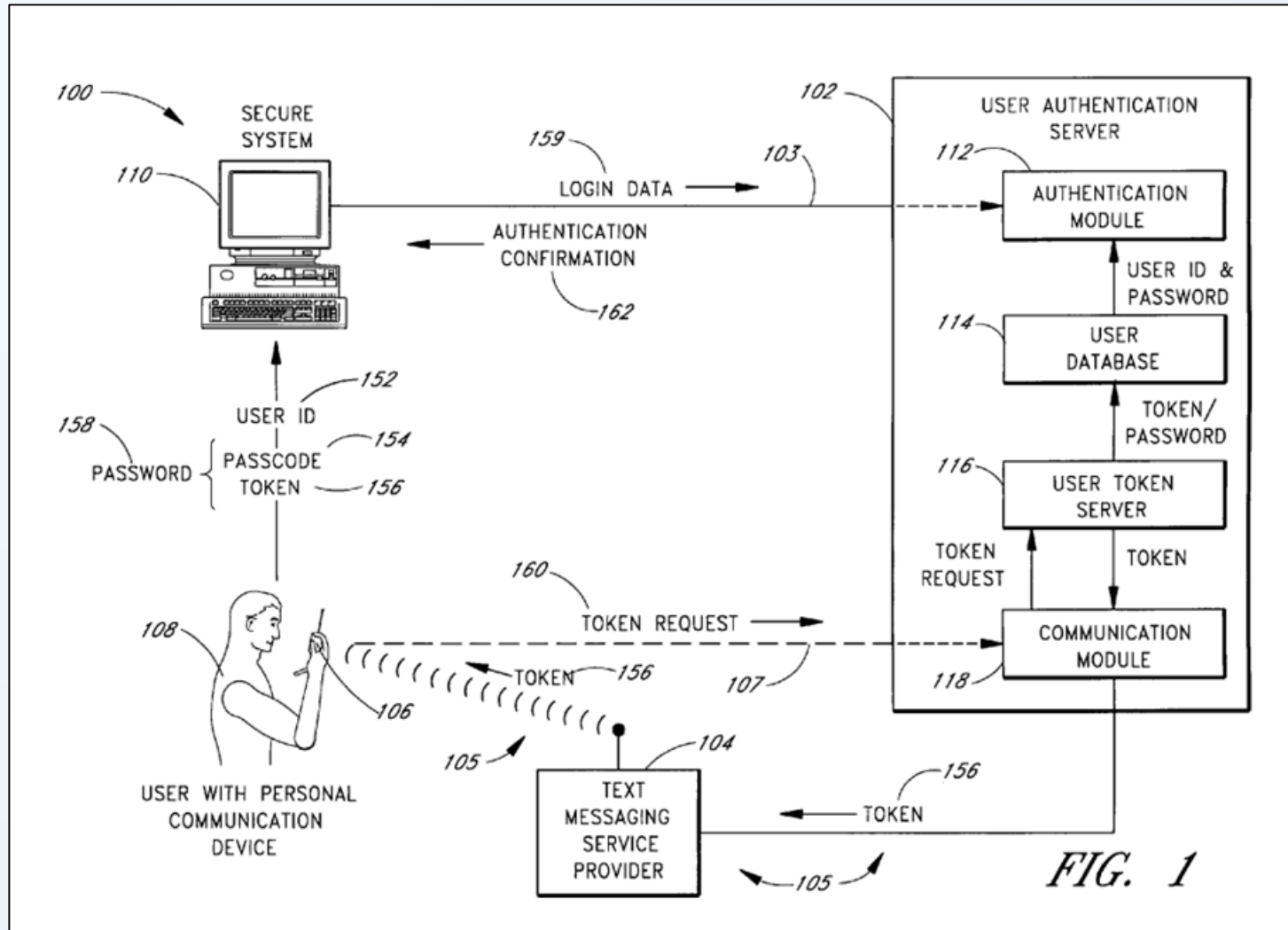


FIG. 1

'658 Patent, Fig. 1

- In the '658 Patent, the "password" is combination of at least the "passcode" and the "token"

Challenged Claims

1. A method of authenticating a user on a first secure computer network, the user having a user account on said first secure computer network, the method comprising:
associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;
receiving a request from the user for a token via the personal communication device, over the second network;
generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting a password associated with the user to be the new password;
activating access the user account on the first secure computer network;
transmitting the token to the personal communication device;
receiving the password from the user via the first secure computer network; and
deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.

3. The method of claim 1, wherein the personal communication device is a mobile phone.

4. The method of claim 1, wherein the personal communication device is a pager.

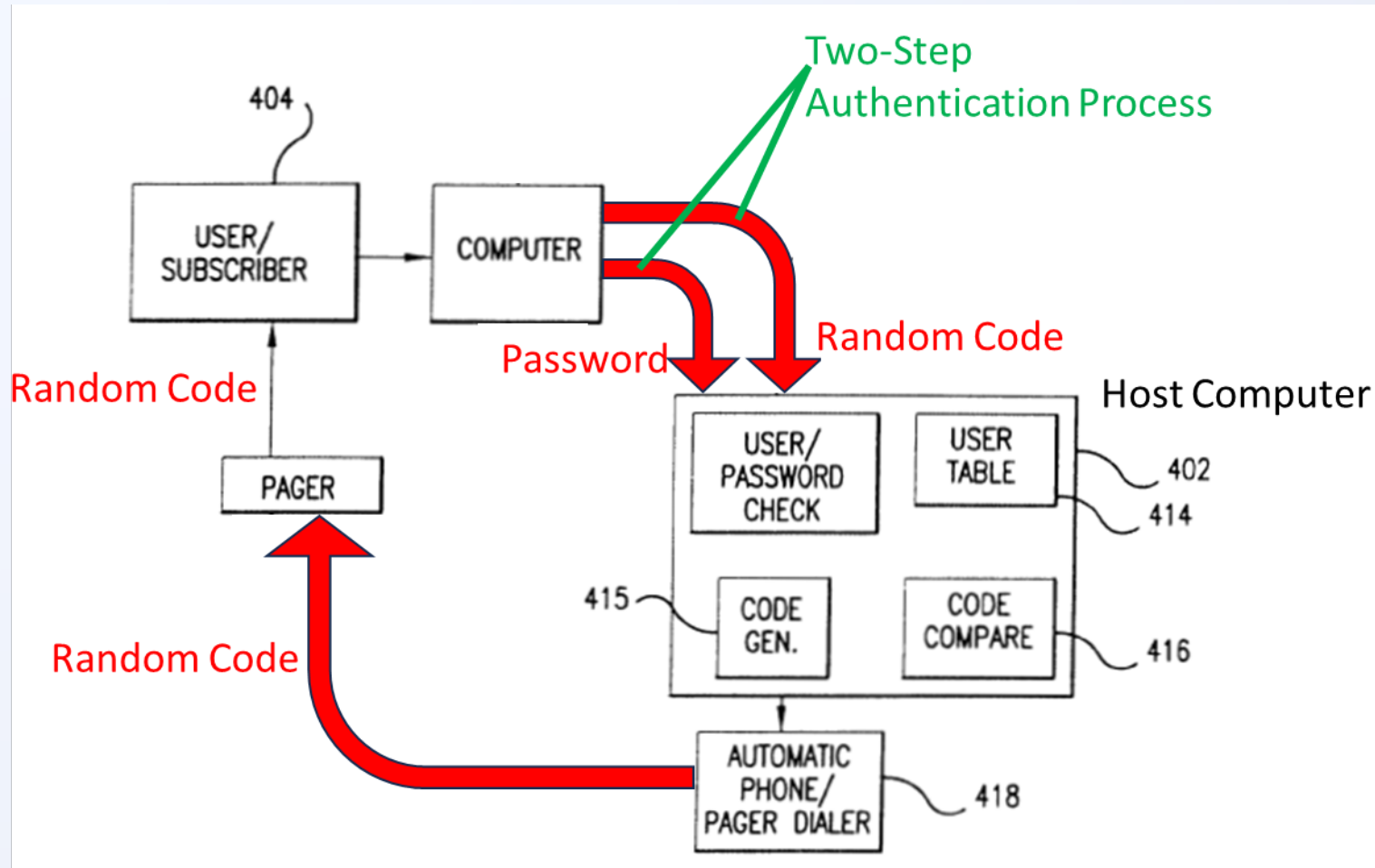
Challenged Claims – Continued

5. A user authentication system comprising:
a computer processor;
a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;
a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;
a communication module configured to transmit the token to the personal communication device through the cell phone network; and

an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

6. The system of claim 5, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.

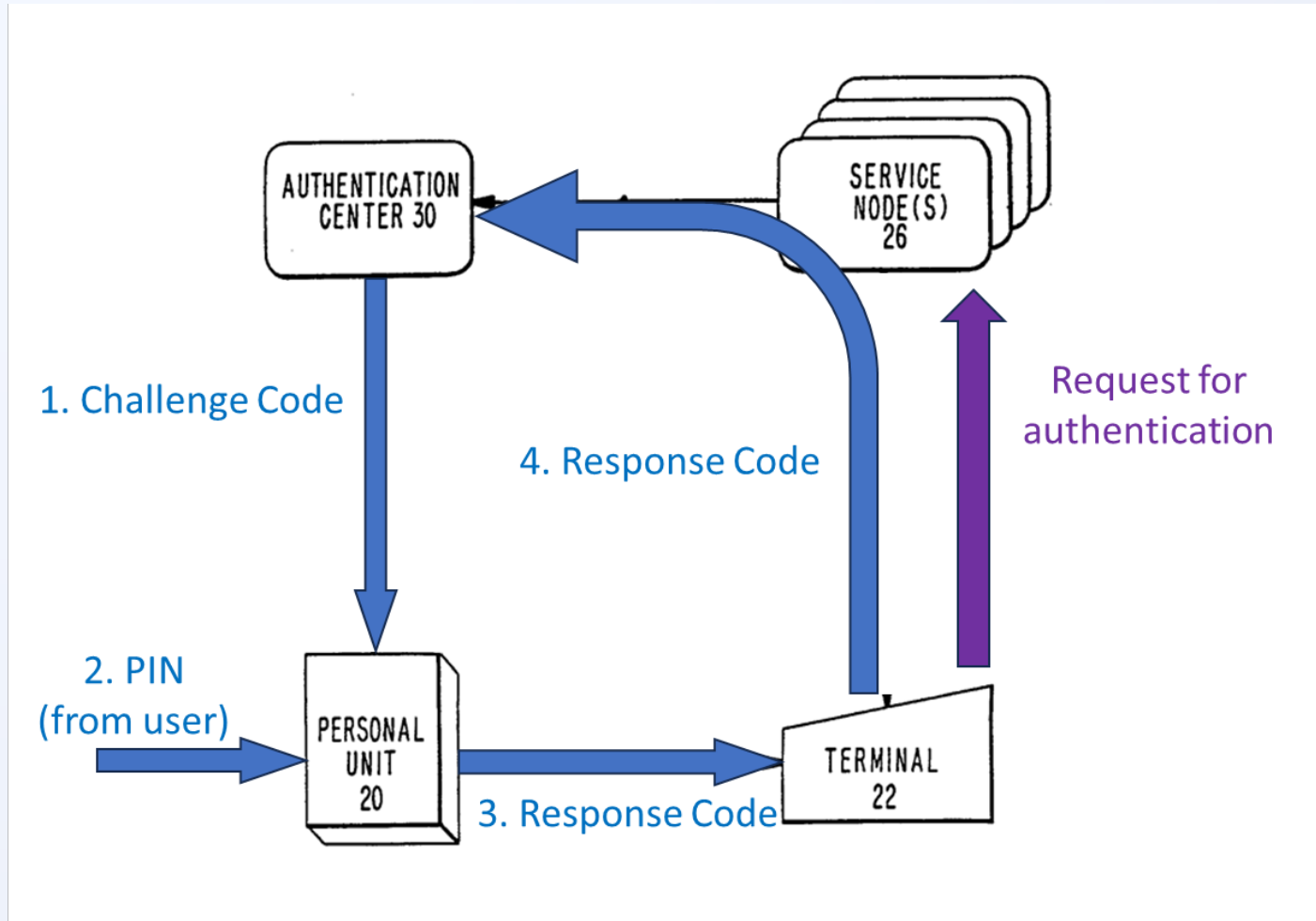
Cited Art *Veneklase*



Veneklase, Fig. 6 (excerpted and annotated).

- *Veneklase*'s password is only transmitted once to host computer.
- *Veneklase* has multi-level security because random code is not generated/transmitted until host computer cross-references received password with a master password list.
- *Veneklase*'s two-step authentication process is a key feature and defines *Veneklase*'s principle of operation.

Cited Art *Jonsson*



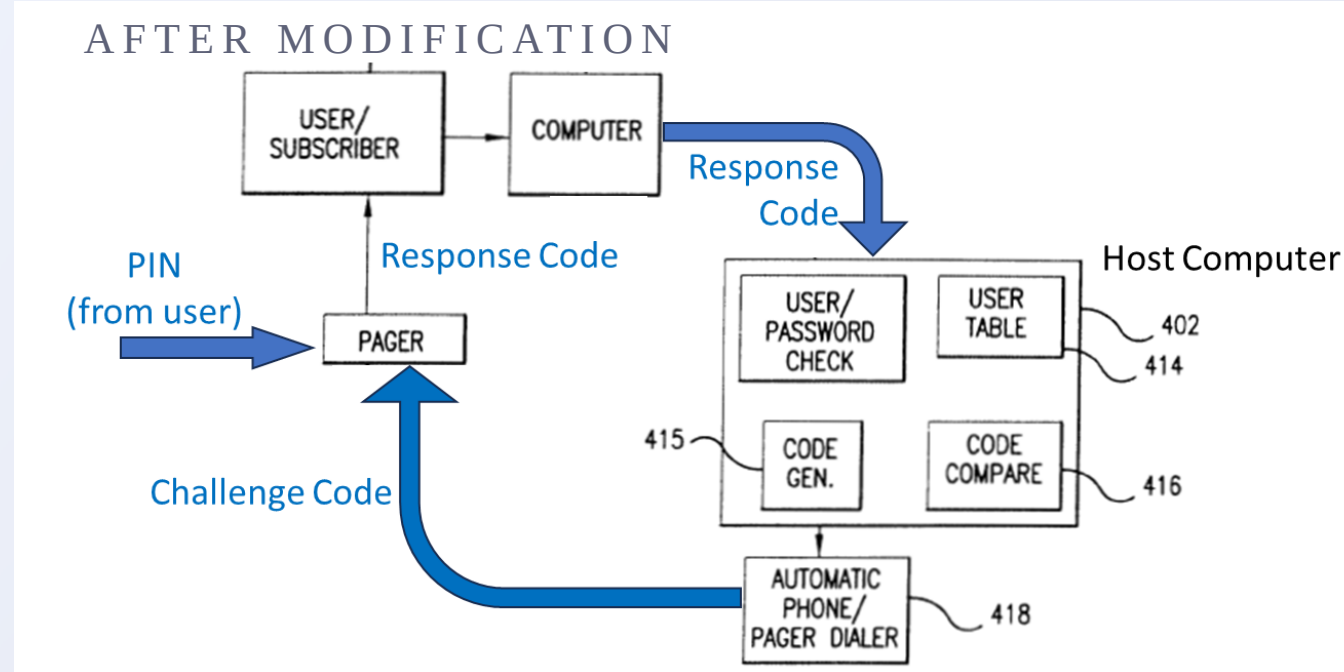
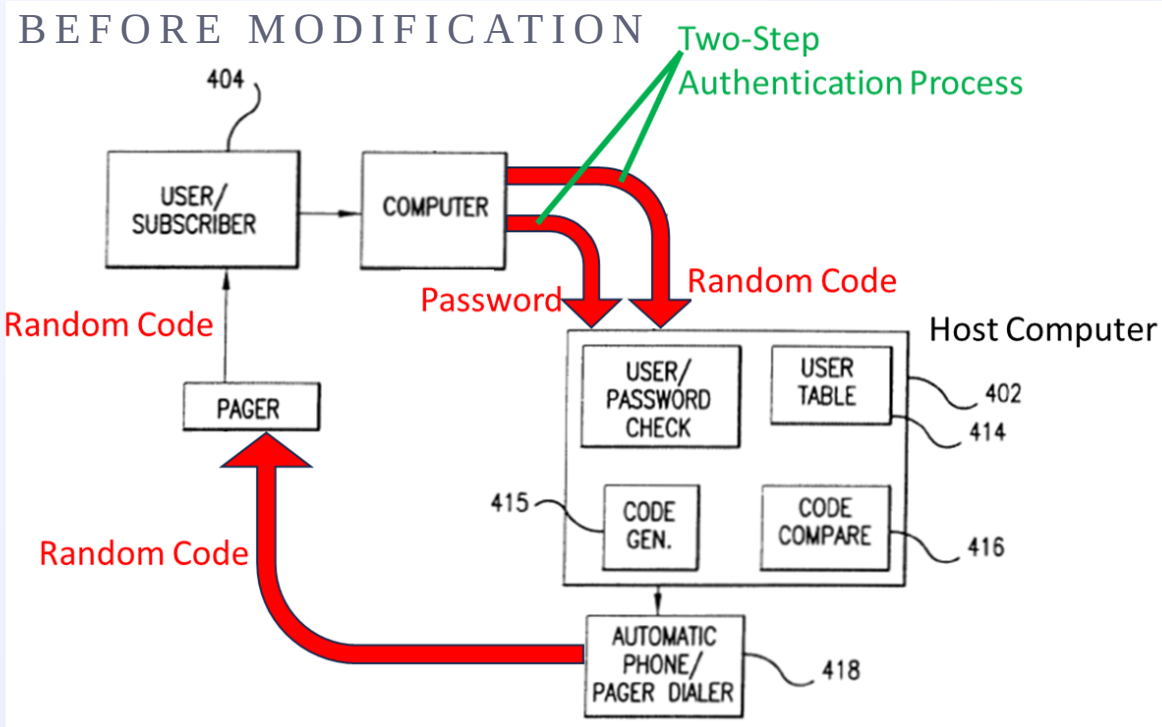
Jonsson, Fig. 1 (excerpted and annotated).

- *Jonsson*'s request for authentication starts authentication process
- "Personal Unit 20" calculates "Response Code" based on "Challenged Code" and "PIN"

Jonsson, 9:1-10:27

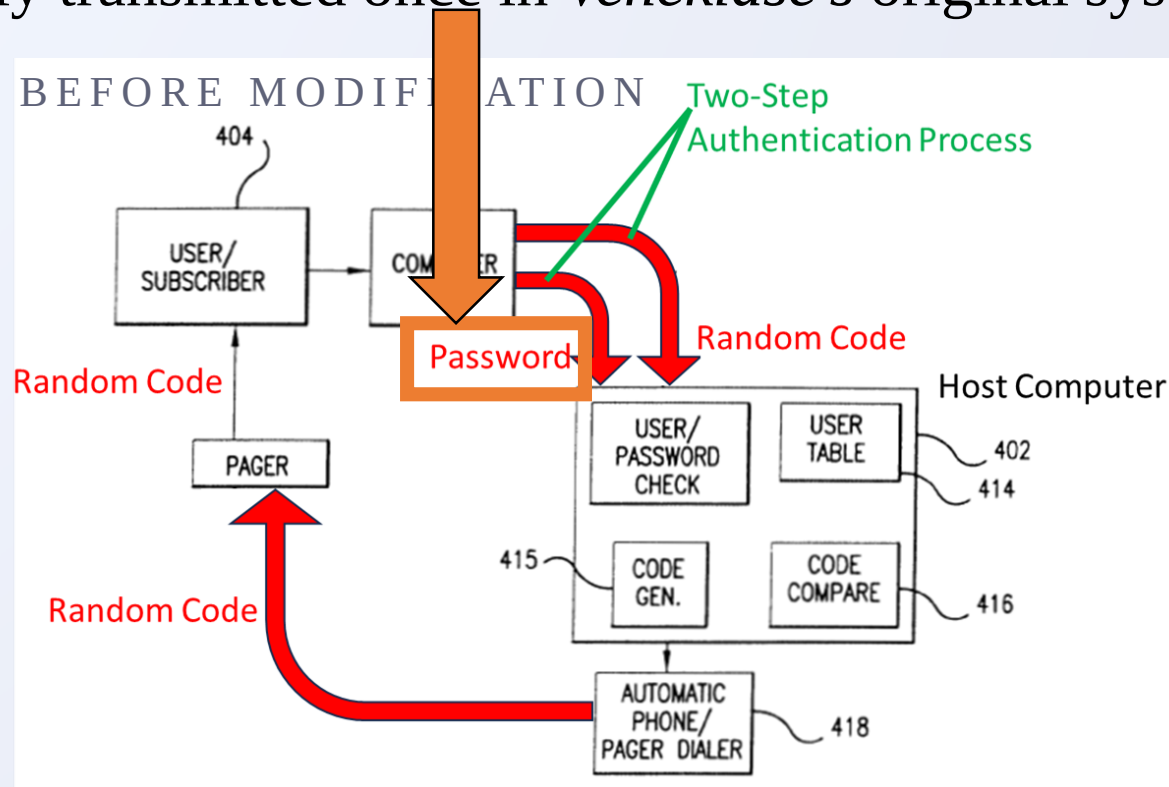
Cited art does not render obvious claim element [5.3] “control module . . . configured to create a new password based upon a token and passcode”

- Petitioner’s modification changes *Veneklas*e’s principle of operation by replacing two-step authentication process
- Petitioner’s modification dismantles *Veneklas*e’s existing multi-level security (e.g., cross-referencing security feature, notification feature)



Cited art does not render obvious claim element [5.3] “control module . . . configured to create a new password based upon a token and passcode”

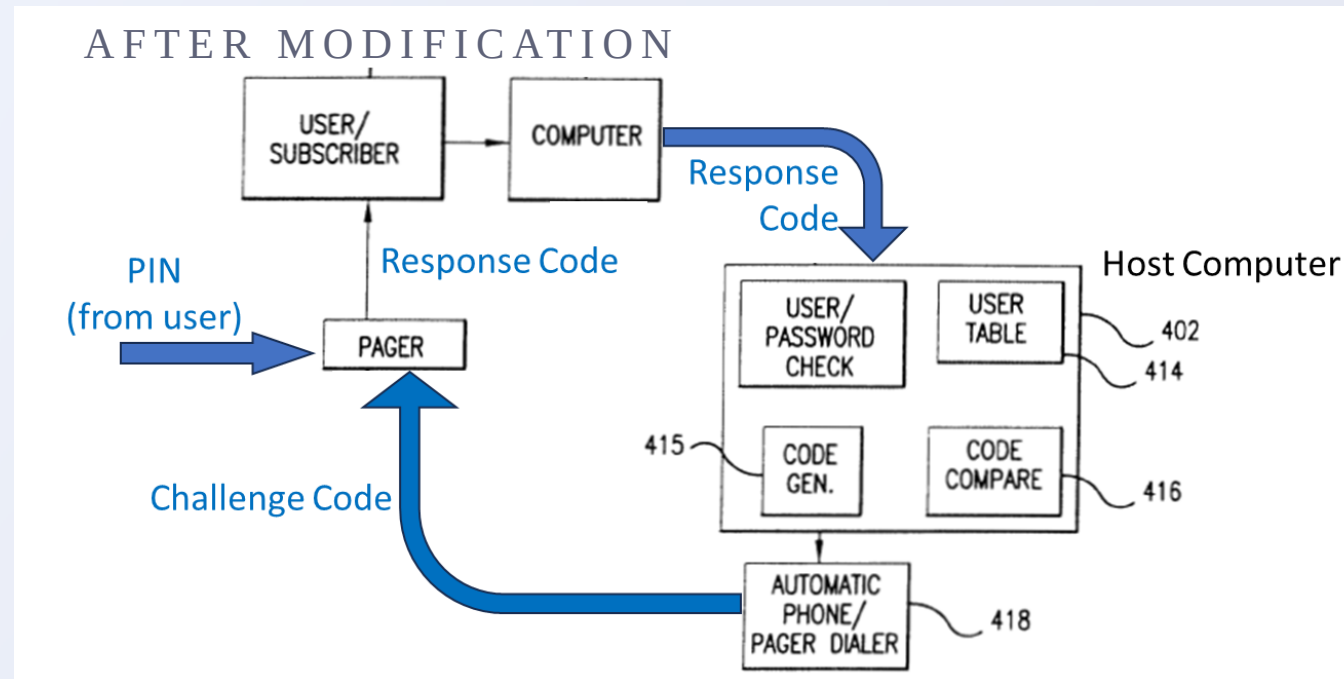
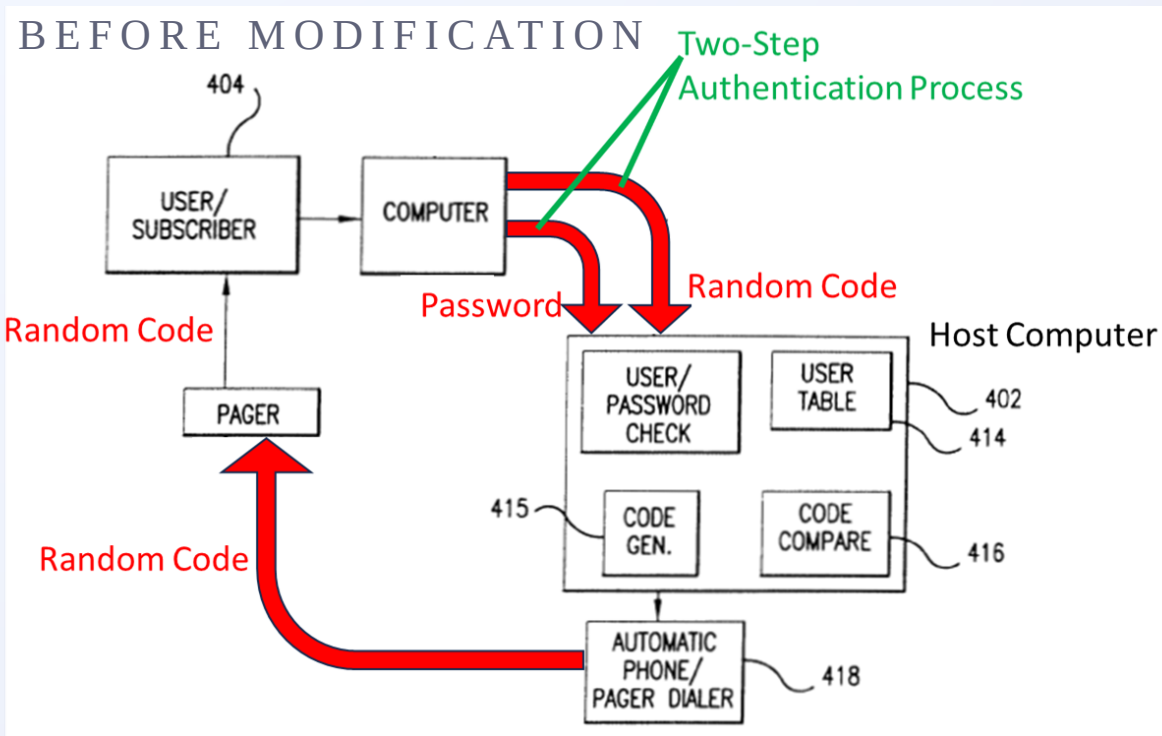
- Alleged motivation to combine: “Jonsson’s use of only a single transmitted password [] allows for enhanced security over the twice transmitted password of Veneklasé.” Reply, p. 6 (emphasis added).
- But the password is only transmitted once in *Veneklasé*’s original system



Veneklasé, Fig. 6 (excerpted and annotated).

Cited art does not render obvious claim element [5.4] “a communication module configured to transmit the token to the” cellphone or pager

- Petitioner’s modification renders *Veneklase* inoperable because password in *Veneklase* is needed to lookup telephone number of cellphone/pager to transmit random code (i.e., step one of two-step authentication process)

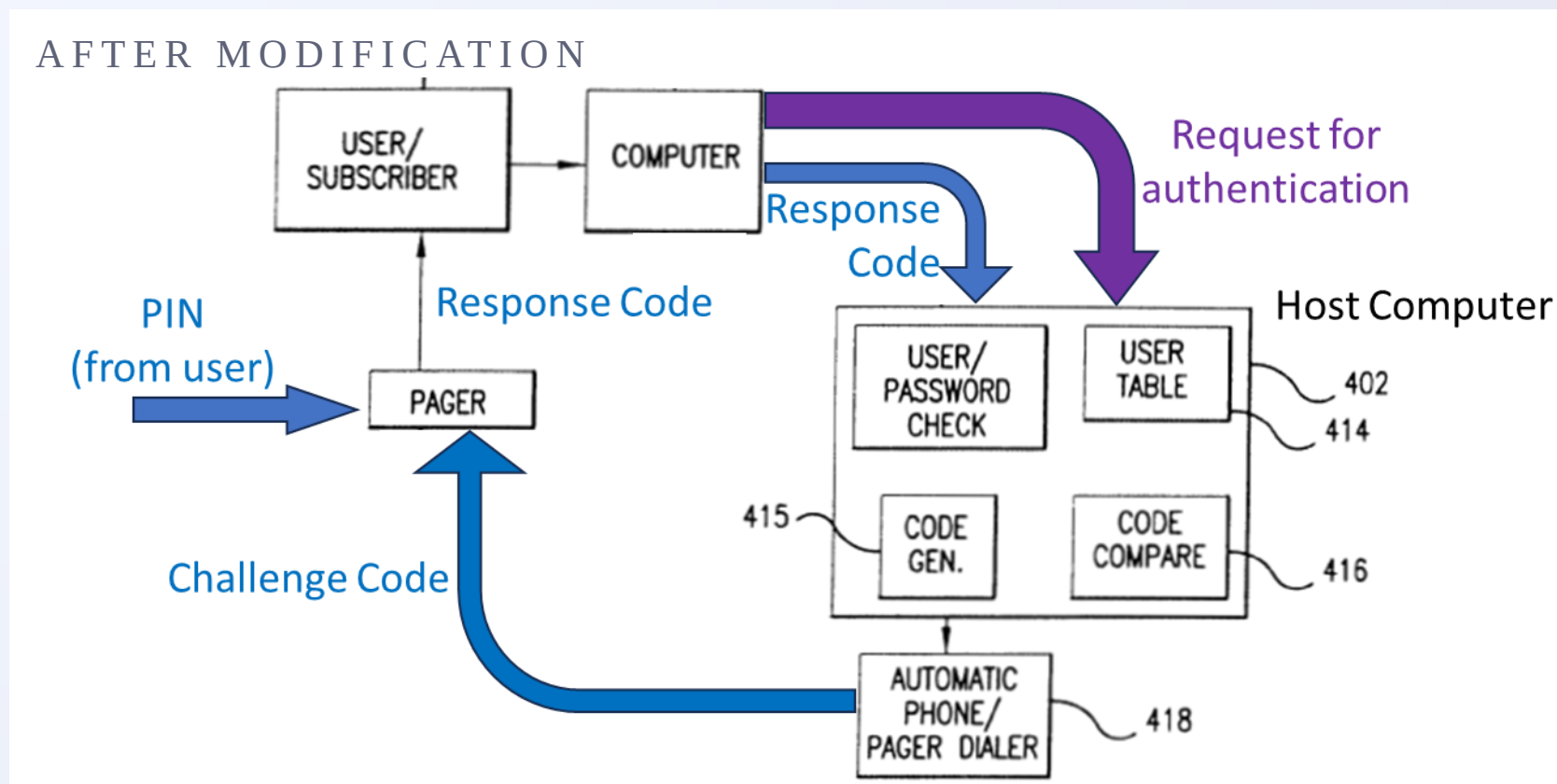


Veneklase, Fig. 6 (excerpted and annotated).

PO Resp., pp. 25-28

Cited art does not render obvious claim element [5.4] “a communication module configured to transmit the token to the” cellphone or pager

- Institution Decision: “the user’s device would be identified in response to the user’s request for authentication as described in Jonsson.” Institution Decision, p. 21.



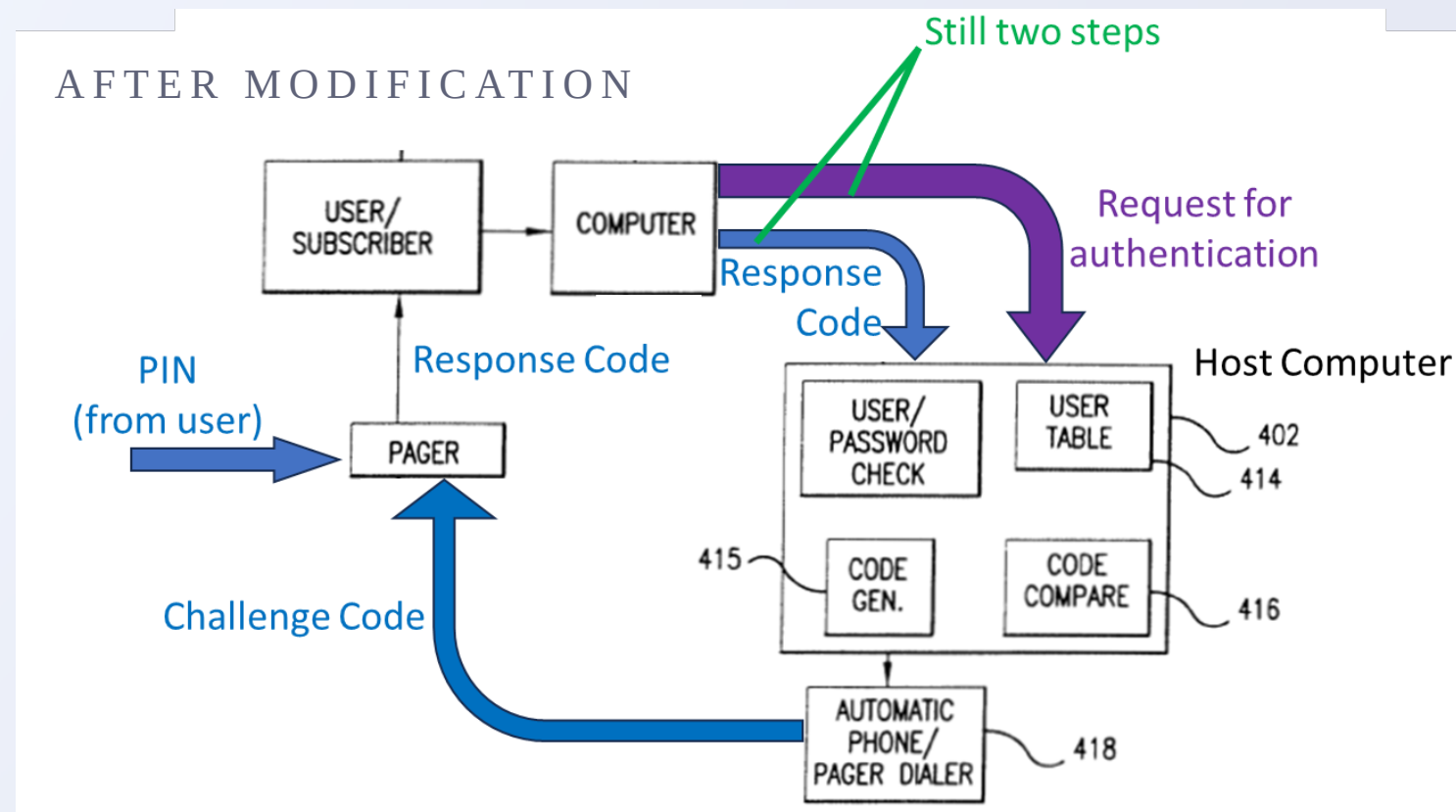
PO Resp., pp. 25-28

Veneklase, Fig. 6 (excerpted and annotated).

Cited art does not render obvious claim element [5.4] “a communication module configured to transmit the token to the” cellphone or pager

- Alleged motivation to combine: “reduc[e] the steps to a single step and thus reduc[e] the amount of time required for the authentication process.” Pet., p. 31
- But proposed combination still has at least two steps (transmit authentication request, transmit response code)
- Proposed combination is more susceptible to DoS attacks

PO Resp., pp. 25-28
Sur-Reply, pp. 5-7



Veneklas, Fig. 6 (excerpted and annotated).

Cited art does not render obvious claim element [5.5] “an authentication module configured to receive the password from the user”

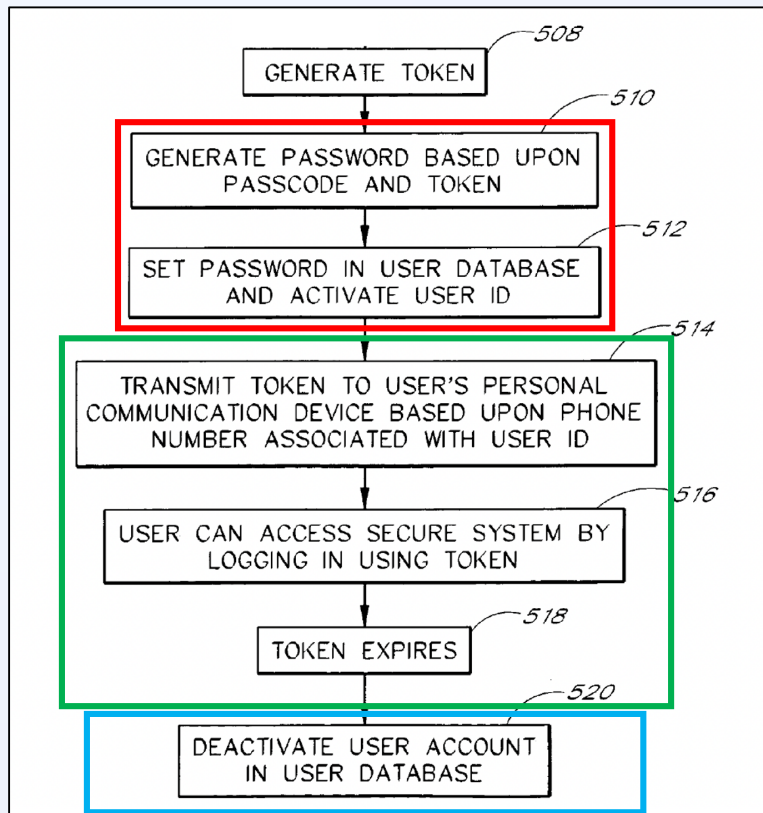
- *Veneklase*’s “pager 420” is off-the-shelf: it only needs to be capable of receiving a message and displaying the message to be ready for use in *Veneklase*’s system
- Petitioner provides no evidence that a user could simply acquire an off-the-shelf pager, in 1996, and immediately start using *Jonsson*’s system without heavy hardware and/or software customization

In a preferred embodiment, the personal unit is a separate unit, thereby minimizing or avoiding the need to customize a communication device such as a cellular telephone. The receiver unit, input device, and the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units, allowing the present invention to be implemented through software.

Jonsson, 7:24-31.

PO Resp., p. 30-31
Sur-Reply, pp. 8-9

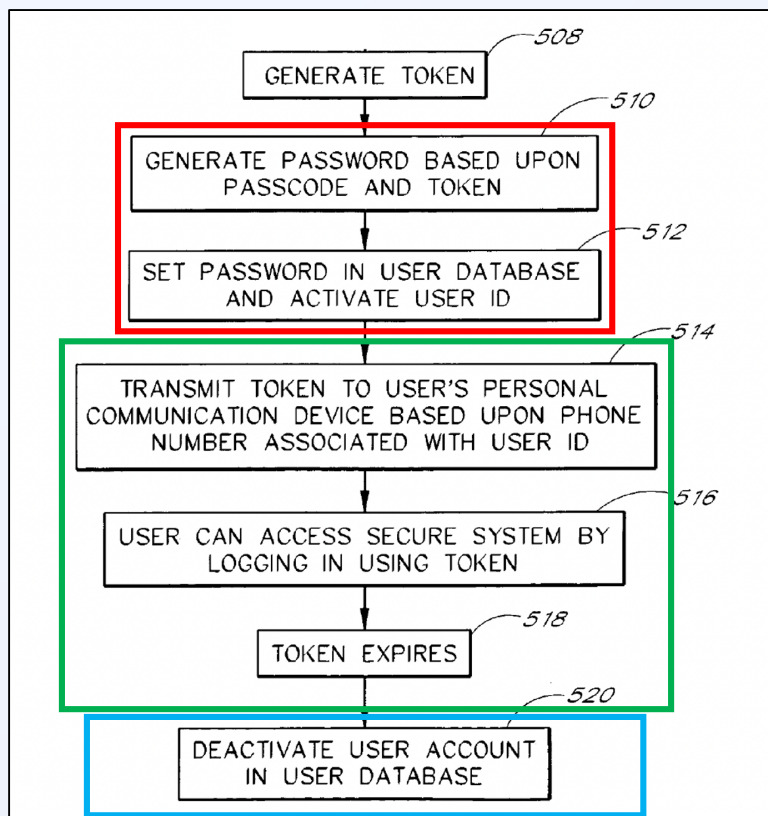
Cited art does not render obvious claim element [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account”



'658 Patent, Fig. 6 (annotated).

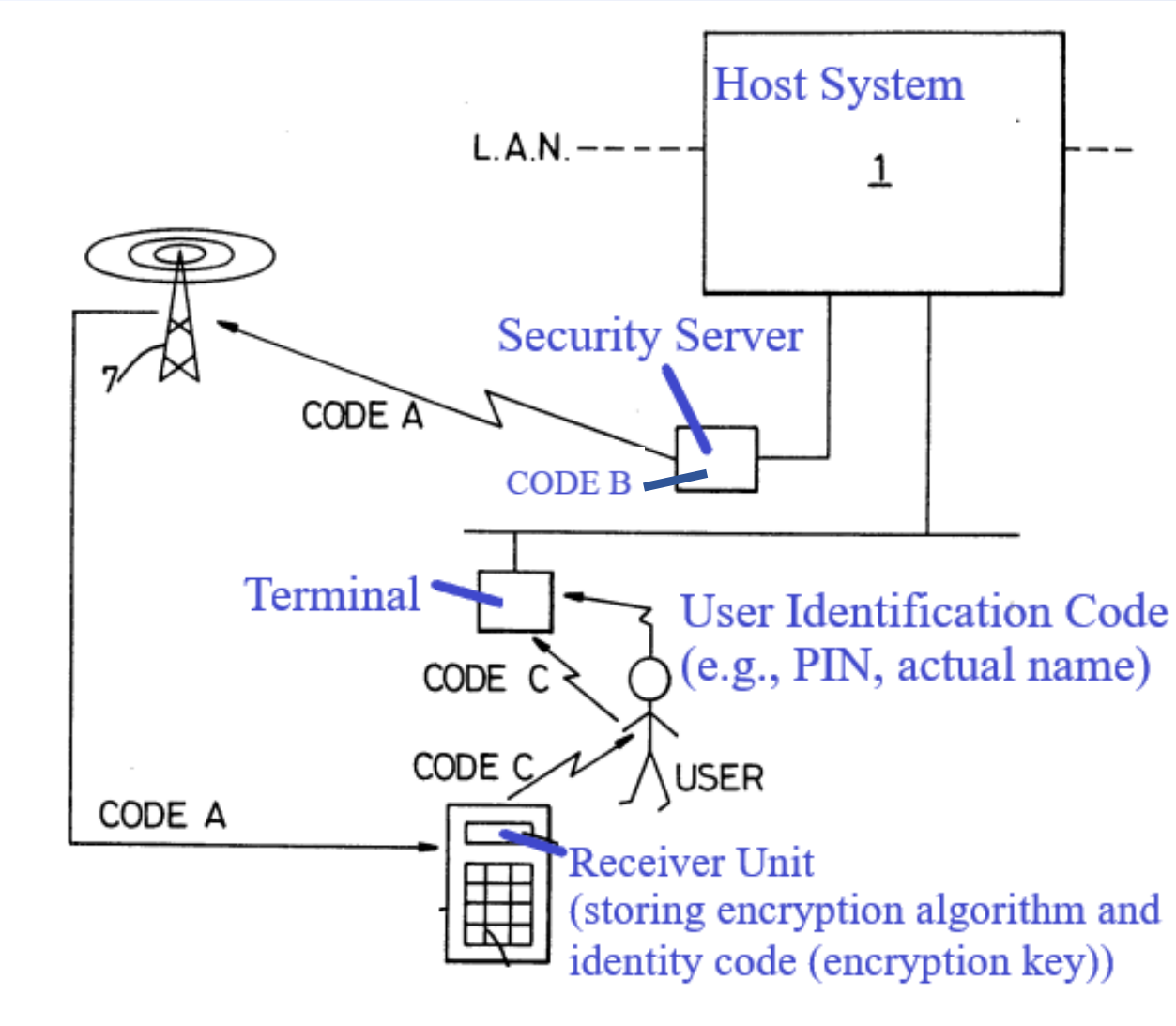
- Claimed “authentication module” activates access to the account in response to creation of the password.
- *Veneklase*’s modified system granting access when received response code matches expected response code is not claimed “activates access.”

Cited art does not render obvious claim element [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account”



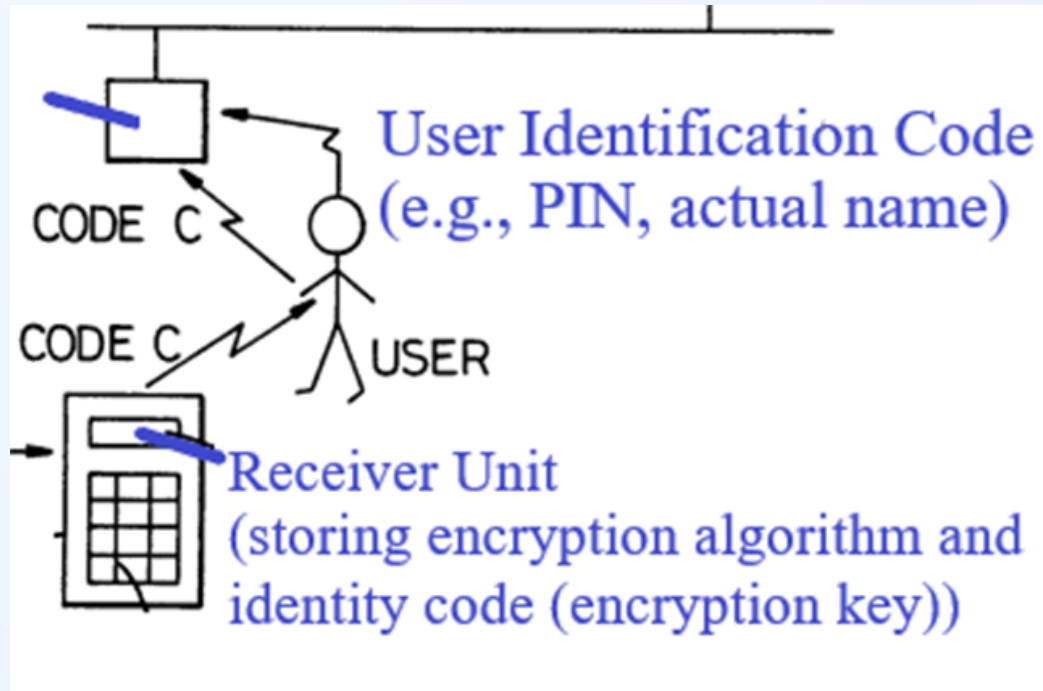
'658 Patent, Fig. 6 (annotated).

- Claimed “activates access” starts a “predetermined amount of time.” The “authentication module” deactivates the account upon expiration of the “predetermined amount of time.”
- The time in *Veneklase*’s modified system between receipt of challenge code and sending back of response code is not claimed “predetermined amount of time.”



Kew, Fig. 1 (excerpted and annotated).

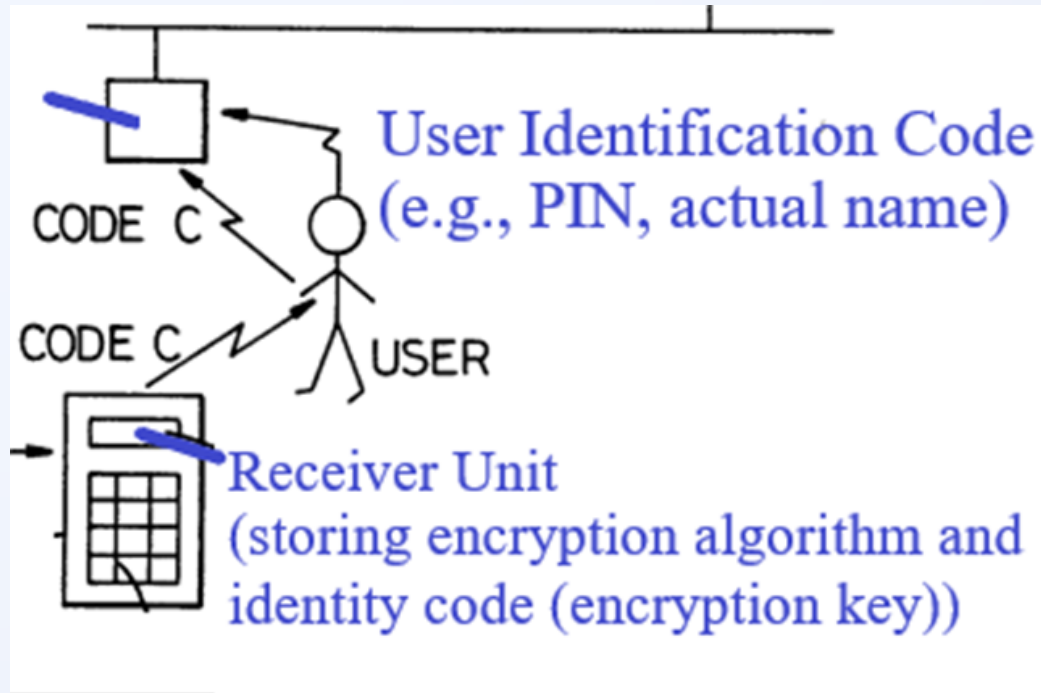
Cited art does not render obvious claim element [5.3] “create a new password based at least upon a token and a passcode . . . known to the user”



Kew, Fig. 1 (excerpted and annotated).

- *Kew*'s "identity code" is an encryption key.
- No evidence that *Kew*'s "identity code" is "known to the user."
- *Kew*'s "identity code" cannot be the claimed "passcode."

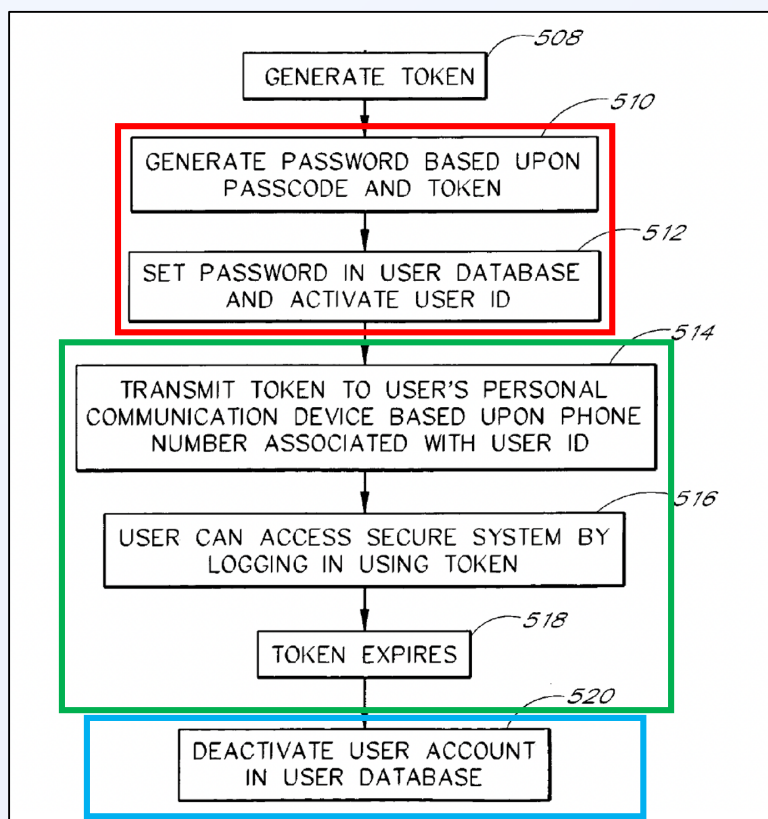
Cited art does not render obvious claim element [5.3] “create a new password based at least upon a token and a passcode . . . known to the user”



Kew, Fig. 1 (excerpted and annotated).

- Petitioner concedes that the claimed “token” and the claimed “passcode” are combined to create the claimed “password”
- “[U]ntil the passcode and token are combined, there is no password.” U.S. District Court (E.D. Tex)
- *Kew*’s “user identification code” is never combined with *Kew*’s “Code A” (Petitioner-identified “token”) and cannot be the claimed “passcode.”

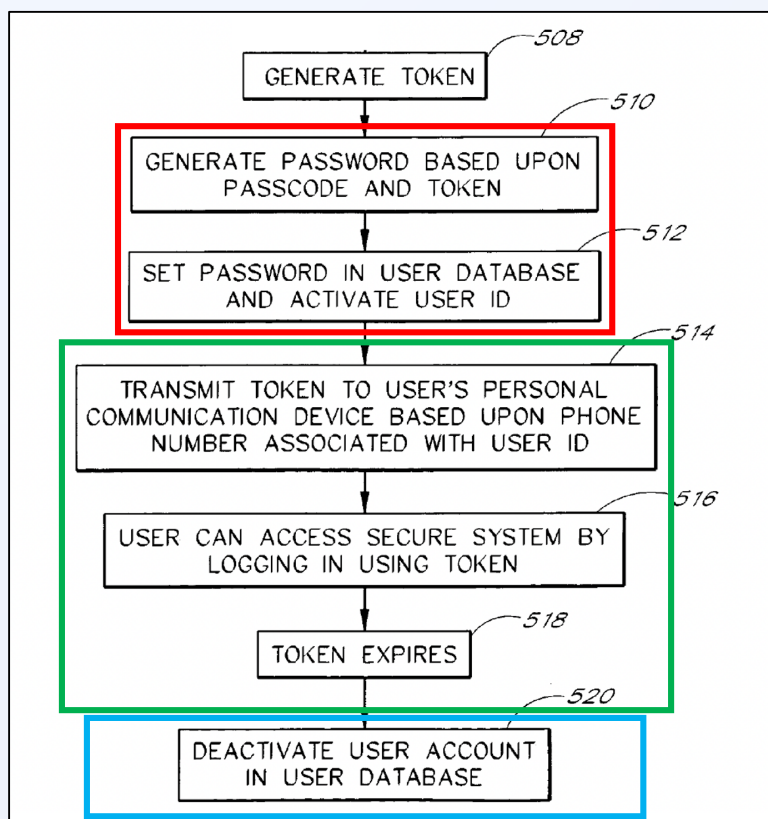
Cited art does not render obvious claim element [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account”



'658 Patent, Fig. 6 (annotated).

- Claimed “authentication module” activates access to the account in response to creation of the password.
- *Kew’s* system granting access when “Code B” matches “Code C” is not claimed “activates access.”

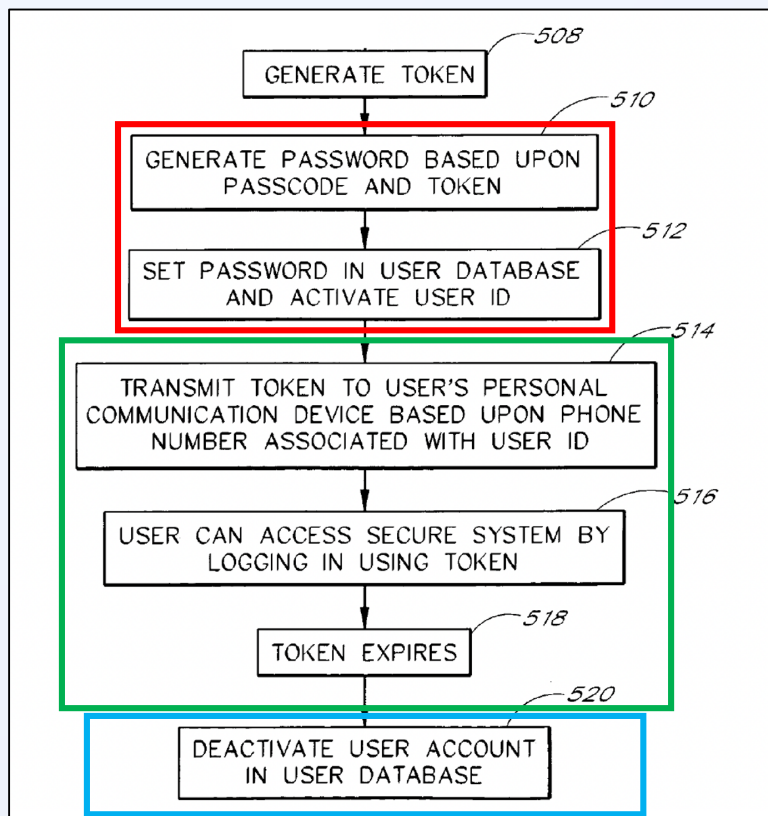
Cited art does not render obvious claim element [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account”



'658 Patent, Fig. 6 (annotated).

- Claimed “activates access” starts a “predetermined amount of time.” The “authentication module” deactivates the account upon expiration of the “predetermined amount of time.”
- In contrast, *Kew’s* “predetermined length of time” starts when “receiver unit” starts displaying “Code C”
- *Kew’s* security server (Petitioner-identified “authentication module”) has no way of knowing when *Kew’s* “predetermined length of time” ends and thus no way of knowing when to deactivate account.

Cited art does not render obvious claim element [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account”



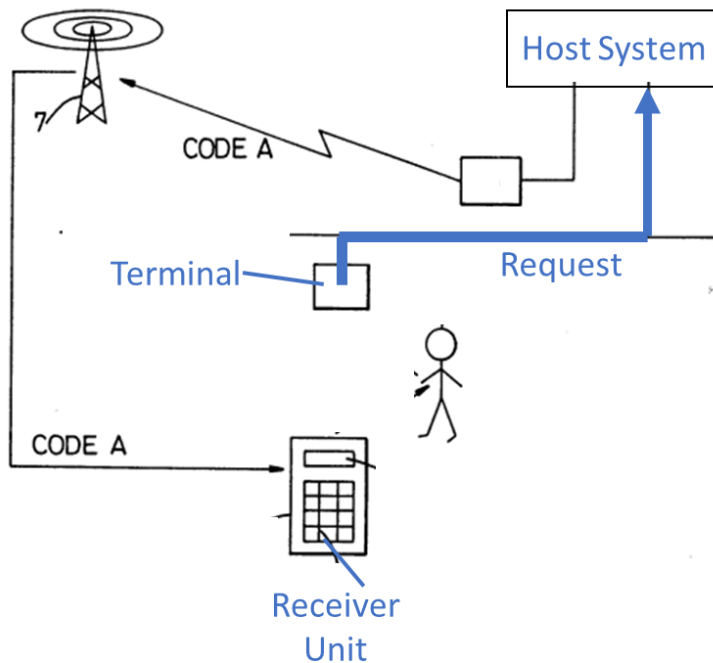
'658 Patent, Fig. 6 (annotated).

- Claimed “activates access” starts a “predetermined amount of time.” The “authentication module” deactivates the account upon expiration of the “predetermined amount of time.”
- In contrast, *Kew*’s “predetermined period” starts when “receiver unit” is activated
- *Kew*’s security server (Petitioner-identified “authentication module”) has no way of knowing when “predetermined period” ends and thus no way of knowing when to deactivate account.

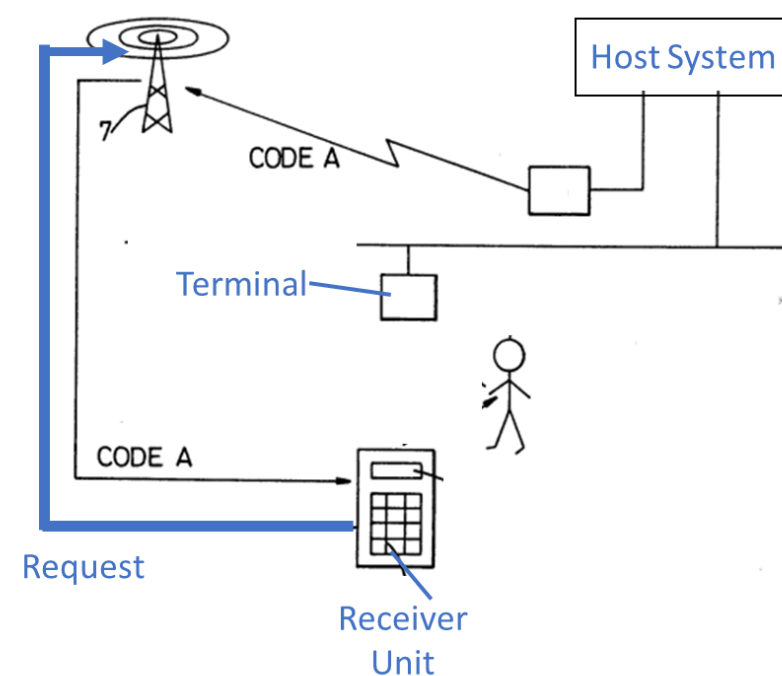
Cited art does not render obvious claim element [1.2] “receiving a request from the user for a token via the personal communication device, over the second network”

- Petitioner’s modification changes *Kew*’s principle of operation
- No evidence *Kew*’s “receiver unit” can transmit anything

BEFORE MODIFICATION



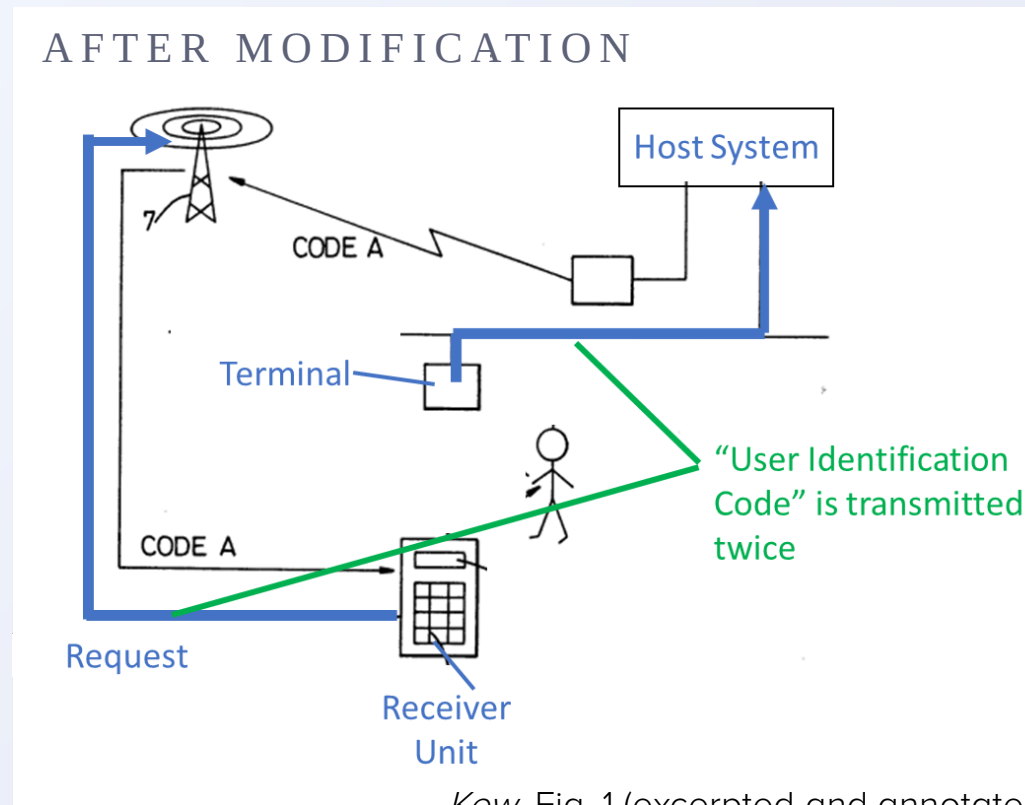
AFTER MODIFICATION



PO Resp., pp. 55-59
Sur-Reply, pp. 24-25

Cited art does not render obvious claim element [1.2] “receiving a request from the user for a token via the personal communication device, over the second network”

- Proposed combination requires transmitting “user identification code” twice, from two separate devices, for single session: risk of interception increased



Kew, Fig. 1 (excerpted and annotated).

Thank you.
