



IPR2023-00425
Unified Patents, LLC
v.
Dynapass IP Holdings LLC
U.S. Patent 6,993,658

Petitioner's Demonstratives
April 16, 2024

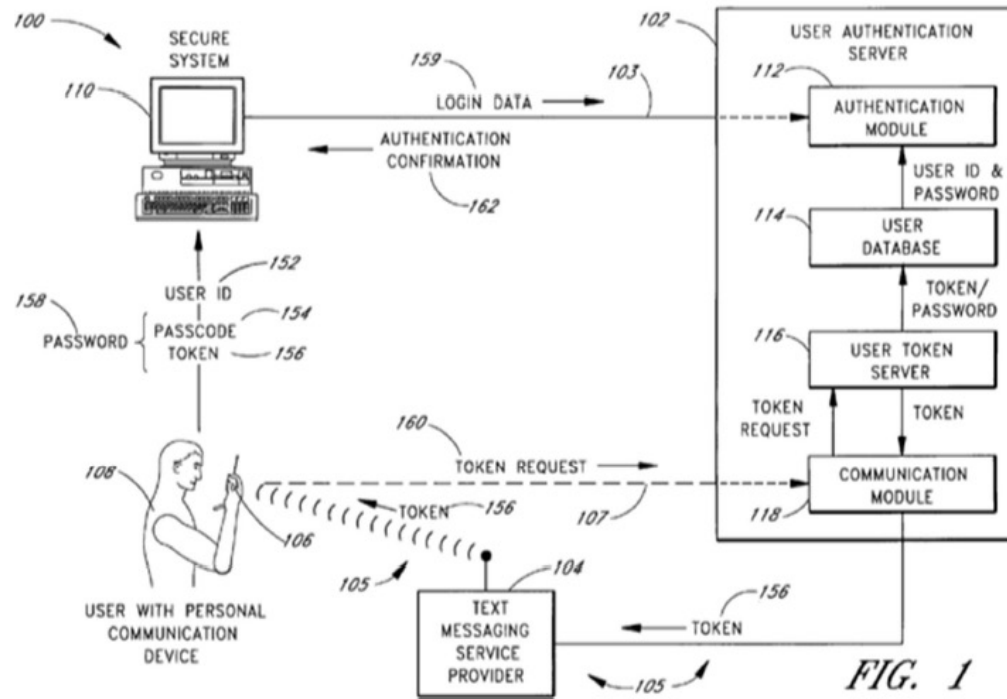
Demonstrative Exhibit- Not Evidence

Petitioner, Slide 1

UNIFIED PATENTS EXHIBIT 1025
UNIFIED PATENTS, LLC v. DYNAPASS IP HOLDINGS LLC
IPR2023-00425

Agenda

- Introduction
- Claim Overview
- Level of Skill in the Art
- Veneklase and Jonsson
- Kew and Sormunen



Ex. 1001, FIG.1

Demonstrative Exhibit- Not Evidence

Challenged Claims

- **Ground 1**
 - Claim 5 would have been obvious over Veneklase (Ex. 1005) and Jonsson (Ex. 1006)
- **Ground 2**
 - Claims 1 and 3-6 would have been obvious over Kew (Ex. 1007) and Sormunen (Ex. 1008)
- PO made no separate arguments with respect to claims 3, 4, or 6.

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:

- [1.1] 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;
- [1.2] receiving a request from the user for a token via the personal communication device, over the second network;
- [1.3] 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;
- [1.4] setting a password associated with the user to be the new password;
- [1.5] activating access the user account on the first secure computer network;
- [1.6] transmitting the token to the personal communication device;
- [1.7] receiving the password from the user via the first secure computer network; and
- [1.8] 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.

5. A user authentication system comprising:

[5.1] a computer processor;

[5.2] 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;

[5.3] 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;

[5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network; and

[5.5] 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,

[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**, such that said account is not accessible through any password via the secure computer network.

Claim Construction

- Limitation [5.6]: “deactivates the account ***within*** a predetermined amount of time ***after*** activating the account”
 - Petitioner/Institution Decision-
 - does **not** require that the predetermined amount of time correspond to the **entire time period between activation and deactivation** of the account. Paper 9, 25.
 - predetermined amount of time **begins at some point after activation**. Reply, 9-10.
 - PO-
 - the claimed ‘predetermined amount of time’ is the timeframe between activation and deactivation of the account. Response at 36.

Claim Construction

- Limitation [5.6]: “activates access to the account in response to the password”
 - PO: activates access to the account in response to **the creation of** the password. Response, 32.
 - Obvious under the plain meaning and PO’s construction. Petition, 41-46, 66-70; Reply, 7-10; 16-17.

Level of Ordinary Skill in the Art

E. Level of Ordinary Skill in the Art

A POSITA for the '658 Patent would have had at least (1) an undergraduate degree in electrical and computer engineering or a closely related field; and (2) two or more years of experience in security. EX1001, generally; EX1003, ¶¶49-51. Petition, p. 5

B. Level of Ordinary Skill in the Art

For the purposes of this Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art ("POSITA") identified in the Petition. Preliminary Response (Paper 8, p. 11)

Petitioner misrepresents that "the Response fails to identify or consider the level of skill in the art." Paper 16, p. 2. In fact, Patent Owner has applied Petitioner's definition of a POSITA throughout these proceedings. See Paper 8, p. 11.

PO sur-reply, p.1

Ground 1 - Claim Limitations in Dispute

5. A user authentication system comprising:

[5.1] a computer processor;

[5.2] 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;

[5.3] 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;

[5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network; and

[5.5] 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,

[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, such that said account is not accessible through any password via the secure computer network.

[5.3] 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;

- Veneklas

- Random Code = token
- Password = passcode

- Jonsson

- Challenge Code = token
- Input security number = passcode
- Response Code = New password

Applicant's foregoing invention is very cost effective as it employs substantially "off the shelf" and readily available components. Further, the use of a "secret" password, a "secret" substantially random number, and a "secret" second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art. 25

Veneklas, Ex. 1005, 7:22-28.

Petition, 25-34

Motivations to Combine

- Transmit one “password” instead of two transmitted “passwords”
- Prevent unauthorized access through SIM swapping
- Explicit teaching, suggestion, and motivation to combine the algorithm of Jonsson because Veneklasen also discloses the use of algorithms for additional security
- Using a known technique to improve similar devices in the same way

Petition, 31-34

Demonstrative Exhibit- Not Evidence

12

5.4- a communication module configured to transmit the token to the personal communication device through the cell phone network;

DoS *n.* Acronym for denial of service attack. A computerized assault, usually planned, that seeks to disrupt Web access. A denial of service attack can occur in a number of forms. The most common form of attack is to overwhelm an Internet server with connection requests that cannot be completed. This causes the server to become so busy attempting to respond to the attack that it ignores legitimate requests for connections. One example of this type of attack, known as a SYN flood, inundates the server's entry ports with false connection messages. Another, known as the Ping of Death, sends a ping command with an oversized IP packet that causes the server to freeze, crash, or restart. Other forms of denial of service attacks include the destruction or alteration of a server's configuration data, such as router information; unauthorized access to physical components of a system; and the sending of large or invalid data that causes a system to crash or freeze. *See also* packet, Ping of Death, SYN flood.

EX1018 (corresponding to EX2005), 173.

Demonstrative Exhibit- Not Evidence

BACKGROUND OF THE INVENTION

A "denial of service" (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DoS attacks are aimed at devices and networks with exposure to the Internet. Their goal is to cripple a device or network so that external users no longer have access to network resources. Without hacking password files or stealing sensitive data, a denial-of-service hacker simply fires up a program that will generate enough traffic to a particular site that it denies service to the site's legitimate users.

EX1019, filed June 21, 2000.

Reply, 3-5

13

[5.5] 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,

Veneklase-

Applicant's foregoing invention is very cost effective as it employs substantially "off the shelf" and readily available components. Further, the use of a "secret" pass-

Ex.1005, 7:23-24.

Jonsson

In a preferred embodiment, the personal unit is a
25 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,
30 allowing the present invention to be implemented through
software.

Ex. 1006, 7:27-31.

[5.6] 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

- Petition

- Activates Access = allow access if received response code matches expected response code. Pet. 41

“The response code is compared to an **expected response code**, which, in exemplary embodiments, may be pre-stored or **generated using the same algorithm and variables.**” Jonsson, 10:2-5

- PO’s interpretation:

- Activates Access = activates access to the account in response to **[the creation of]** the password

“the challenge code and the response is **unique for each transaction.**” Jonsson, 3:16-18

Petition, 41-46; Reply, 7-10.

[5.6] 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

40 In operation, timing means 40 records the time at which the first and second passwords are received by analyzing means 12. Timing means 40, in one embodiment which is coupled to analyzing means 12 and code generation means 14 by bus 42 and in another embodiment which is in software communication with means 12 and 14, then compares the times to determine whether the second password was received within a predetermined period or **predetermined "window" of time after the first password was received**. In the preferred embodiment...

Veneklase, 8:40-49

to receive the code. **If the second password was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g.**

Veneklase, 9:3-5.

Veneklase-Jonsson

- “predetermined ‘window’ of time”
 - Receive/send challenge code
 - Send response code for comparison to expected response code

Petition, 42-46; Reply, 7-10.

Ground 2 - Claim Limitations in Dispute

5. A user authentication system comprising:

[5.1] a computer processor;

[5.2] 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;

[5.3] 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;

[5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network; and

[5.5] 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,

[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, such that said account is not accessible through any password via the secure computer network.

Ground 2 - Claim Limitations in Dispute

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:

[1.1] 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;

[1.2] receiving a request from the user for a token via the personal communication device, over the second network;

[1.3] 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;

[1.4] setting a password associated with the user to be the new password;

[1.5] activating access the user account on the first secure computer network;

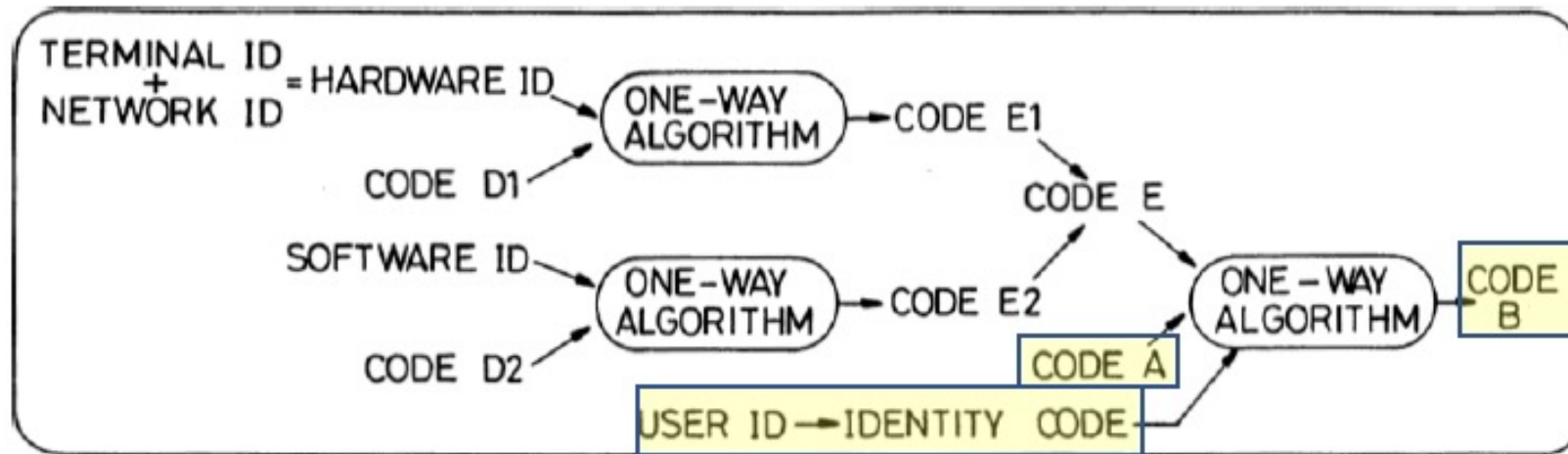
[1.6] transmitting the token to the personal communication device;

[1.7] receiving the password from the user via the first secure computer network; and

[1.8] 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.

[5.3] 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;

- UserID/Identity Code = passcode
- Code A = token
- Code B = New Password



Pet. At 60-62; Ex. 1007, FIG 2

Demonstrative Exhibit- Not Evidence

19

[5.3] 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;

Claim 1: A method of preventing unauthorised access to a host computer system (1) by a user at a remote terminal (2) comprising the steps of

accepting a **user identification code [passcode]** input to the terminal by the user;

generating a random code (Code A) [token] ;

subjecting Code A to a transformation characteristic of a transformation algorithm **identified by the input user identification code** so as to generate a transformed code **(Code B) [New Password]**; transmitting Code A via a paging system (7) , to a receiver (6) held by the user, the receiver (6) comprising transformation means adapted to transform the received Code A to a second transformed Code C...

When the user seeks access to the host system 1 via the terminal 2 , **he enters his user identification code**. This code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN. The security server 5 includes a database of all authorised users and their authorised receiver units 6, and **identifies the corresponding identity code** for the appropriate receiver unit 6. **The security server 5 then generates a random code (Code A)** and subjects this number to an encryption **using the same one-way algorithm as is stored in the user's receiver 6 together with the corresponding identity code**. In this way a transformed code (Code B) is produced. EX1006, 7:34-8:10

[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, such that said account is not accessible through any password via the secure computer network.

- Petition
 - Activates Access = allows access to the account by the user (Code B and Code C match)
- PO's interpretation:
 - Activates Access = activates access to the account in response to **[the creation of]** the password
- Kew discloses creation of Code B (new password) when sending Code A (token) to the receiver to be transformed to Code C, which is then compared to Code B to allow access to the account
 - POSITA would have understood account access to be activated under PO's interpretation when Code B was created and not after code C was received for comparison to Code B

Petition, 41-46; Reply, 7-10

[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**, such that said account is not accessible through any password via the secure computer network.

- Kew discloses that the security server “**prompts**” entry of the “transformed Code C **displayed by the receiver unit 6.**” EX1007, 9:6-7.

Code C is then displayed to the user on a display means 9, preferably a liquid crystal display, for a predetermined length of time such as five minutes.

5 The terminal 2, at the behest of the security server 5
prompts the user to input the transformed Code C displayed
by the receiver unit 6. After input, the security server 5
compares the input Code C with the transformed code, Code
B, it produced by encryption of the random code, Code A. If
10 Code B and Code C are identical, access to the host system
1 is permitted.

prompt n. 1. In command-driven systems, one or more symbols that indicate where users are to enter commands. For instance, in MS-DOS, the prompt is generally a drive letter followed by a greater than symbol (C>). In UNIX, it is usually %. *See also* command-driven system, DOS prompt. 2. Displayed text indicating that a computer program is waiting for input from the user.

EX1018, 427; EX1024, ¶35

Petition, 48, 62, 64, 66; Reply 17-22

Demonstrative Exhibit- Not Evidence

22

Time-Bound Access was well-known in the art decades before the earliest priority date

C. Time-bound access

49. The concept of time-bound access in secure systems is almost as old as the design of security systems. As an example, it is commonplace for systems that use cryptographic keys to “age” the keys as they are used. The principal reason for this is that the longer a cryptographic key is in use, the more information that depends on the security of that key will be transmitted and thus, the likelihood that an attacker will gain an advantage in breaking the security of a cryptosystem. In the worst case, if an encryption key is completely compromised, all the information transmitted using that encryption key will also be compromised. By restricting the time period for which the same cryptographic key is used, the loss of information can be mitigated. Also, in theoretical terms, any knowledge that an attacker may

Kew's time-bound access

The receiver unit 6 therefore uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm. This transformed **Code C is then displayed to the user on a display means 9**, preferably a liquid crystal display, **for a predetermined length of time** such as five minutes. Kew, 8:33-9:3

the receiver can only be **enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C** by input of a second user identification code by the user. This second code may also be in the form of a PIN. In this way additional security is provided since an unauthorised user cannot gain access to the system even if he has possession of the receiver and knows the user identification code without knowledge of the second identification or activation code. Kew, 3:14-23

Kew's time-bound access as understood by a POSITA

- 1) The user enters the user ID to generate Code A, which is used with the user ID/identity code to generate Code B, which begins the lifetime of Code B for a predetermined 5 minute period.
- 2) Code A is sent to the receiver, which begins the lifetime of Code A for a predetermined period of 5 minutes.

The user is alerted to enter his second identification code, which enables Code A to be transformed to Code C and displayed.
- 3) The user must enter Code C while it is displayed during the 5 minute period that the receiver is enabled to generate code C.

Reply, 22; EX1024, ¶39.

PO: Kew's "security sever" (Petitioner-identified "authentication module") has no way of knowing when Kew's "receiver unit" stops displaying "Code C," and thus has no way of knowing when to deactivate the account. Sur-reply at 23.

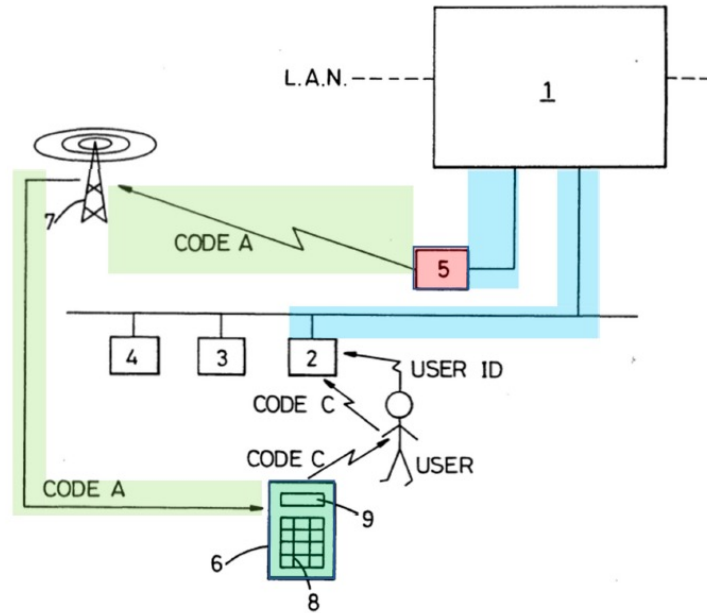
- Allows Code C to be valid indefinitely
- Does not prevent a user from simply writing down Code C and entering it days later to access the account
- Ignores the "prompt" from the security server

Reply, 17-21



Demonstrative Exhibit- Not Evidence

[1.2] receiving a request from the user for a token via the personal communication device, over the second network;



Kew, Fig.1

Petition, 74-75; Reply, 23-24

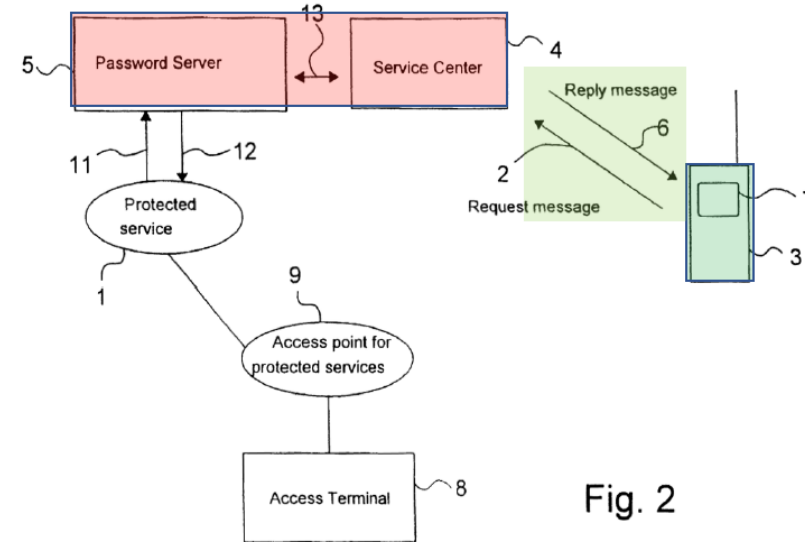


Fig. 2

Jonsson, Fig. 2

Kew's receiver is linked to the remote terminal for the exchange of information

the receiver unit 6 would probably, but not necessarily, comprise a stand-alone piece of equipment, in this embodiment **the receiver unit 6 is intended to be linked to the remote terminal 2 for the passage of information therebetween**

Kew, 9:27-31; EX1024, ¶40; Reply, 23

