(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69884 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/04481

(22) International Filing Date: 12 February 2001 (12.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/525,806 15 March 2000 (15.03.2000) US

(71) Applicant *(for all designated States except LC)*: **NOKIA MOBILE PHONES LIMITED** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: **LUKKAROINEN, Mikko**; Telkkatie 4B, Fin-90150 Oulu (FI). **INGET, Virve**; Takavainiontie 9 A7, FIN-90560 Oulu (FI).

(74) Agent: **GREEN, Clarence, A.**; Perman & Green, LLP, 425 Post Road, Fairfield, CT 06430 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

WO 01/69884 A2

(54) Title: SECURE USER ACTION REQUEST INDICATOR

(57) Abstract: A mobile communications device is adapted to use applications resident on a remote network server. The display of the mobile device is divided into static and dynamic display zones. Inquiries originating externally from the mobile device are identified and restrictively routed only to the dynamic display. Internally generated inquiries trigger an indicator symbol within the static display. In this manner bogus requests for confidential identifiers may be avoided.

# SECURE USER ACTION REQUEST INDICATOR

## Background of the Invention

Communications devices, such as mobile phones, pagers and the like, are being packed with more and more features. In the past such mobile equipment has been a closed environment namely, all of the features use software within the mobile equipment or SIM. With the advent of new technologies, which use wireless communications protocols, such as Wireless Application Protocol (WAP) or comparable protocols, additional applications are accessible by the mobile device, from network servers. As a result a new security threat arises for mobile equipment. Mobile equipment will soon be subject to queries designed to extract confidential security information from the user, such as a PIN or other identifier. It is therefore necessary to devise a reliable system in which requests for information originating from remote "hostile" sources can be readily identified, ignored.

It is a purpose of this invention to provide a system for identifying remote inquiries which may precipitate a breach of security in the use of mobile equipment such as a mobile telephone, pager or other similar communications device.

## Summary of the Invention

In order to use applications accessible from a network server, a mobile device is designed for

interactive use. This enables the mobile device to run such applications stored on a network server remote from the mobile device. To reduce the risk of receiving bogus requests for confidential identifiers, a system is designed to identify externally generated inquiries. To this end, means are provided to segregate the display of remote information requests. The mobile device is equipped with a display that is divided into dynamic and static display zones. Externally generated inquiries can be written only to the dynamic zone. Internally generated inquiries will trigger an indicator in the static zone to advise the user of the authenticity of the inquiry. As a result hostile requests for information may be immediately recognized and ignored.

**Description of the Drawing**

The invention is described in more detail below with reference to the attached drawing in which:

Figure 1 is a block diagram of a communication system utilizing the subject invention;

Figure 2 is a information flow diagram of the method of this invention; and

Figures 3a and 3b illustrate embodiments of the segregated screen of this invention.

**Description of the Preferred Embodiment**

The basic components of the communications system of this invention are shown in the block diagram of figure 1. A mobile device 1 is connected through a communications link 9 to a network server 10. In this instance, the network server 10 does more than facilitate communications traffic, it also provides interactive applications such as banking, E-mail, investing and other features.

Mobile device 1 includes a microprocessor control unit (MCU) 2 that is accessed by the user via a user interface 3, such as a keyboard. Display 5 communicates information from the MCU 2 to the user. The MCU 2 contains the required software or firmware to execute the functions on mobile device 2 required to operate the applications resident in the network server 10. Many of the applications will require the use of security identifiers, such as PINS and other confidential codes to be access the personal application files of the user.

In the early days of networked computers, there was a proliferation of bogus log-in procedures that generated inquiries to the personal computer for confidential information. If the information was supplied, it was stolen and used for criminal or other activities not authorized by the user. The risk of such security breaches is now becoming a problem for the user of mobile devices, especially those equipped to take

advantage of the communications protocols such as WAP. Such protocols represent standard operating procedures for interactive transmittal of data used to execute an assortment of transactions. Although many of these transactions are secure because of the required digital signatures, such as PIN codes, it is essential that the code be maintained confidential. Bogus inquiries are a significant threat to the usefulness of these applications.

The mobile device 1 of this invention is equipped with a display 5, which is divided into two discrete zones, a static display zone 7 and a dynamic display zone 6. An internal display router 4 directs internally generated inquiries and information to either the static or dynamic displays.

As shown in figures 3a and 3b, the static display 7 may present menu icons, tool symbols, status indications, such as battery level, and other administrative references. The dynamic display 6 is for displaying interactive information relative to executing the activities of an application in progress. Information generated within the mobile device, may be displayed on either the static or dynamic displays.

Information transmitted to the mobile device 1 from, for example a hostile source 11 through the network server 10, will utilize browser protocols and be readily identifiable. This information is directed to the dynamic display 6 by a external display router 8. In this manner, information from the network server 10

is isolated from the internally generated information of the mobile device 1.

To inform the user of the authenticity of inquiries for identifier codes, an indicator symbol 12, for example a blinking icon, will be displayed in the static display 7, as shown in figures 3a and 3b. When displayed, this symbol will indicate to the user that the request is internally generated. Since the MCU identifies the external inquiry and this information is only routed to the dynamic display 6, there is a reliable indication that a PIN number can be transmitted without appreciable risk of abuse.

As shown in figure 2, in operation, if a bogus log-in procedure from hostile source 11 is transmitted through the network server 10, when it is received, it is identified by the MCU and routed only to dynamic display 6. The externally generated inquiry may be written only to the dynamic display 6. When an inquiry is generated by the execution of internal software, an indication is prominently displayed in the static display 7. When responding to the inquiry displayed in dynamic display 6, the user will be warned not to respond unless the internal indicator is displayed.

In this manner transmittal of confidential identification codes, restricted and the risk of unauthorized interception and use of PIN codes and the like may be significantly reduced.

We claim as our invention:

1. In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, a system within said mobile device for indicating the authenticity of inquiries for confidential identity codes comprising:

a control processor for operating said mobile device, said processor adapted to identify said inquiries for confidential identity codes as externally generated or internally generated;

a display for presenting information to the user, said display divided into first and second display zones; and

routing means constructed to send externally generated information only to said first display zone;

wherein said control processor generates an indication symbol in said second display zone when the inquiry is internally generated to indicate to the user that said inquiry is authentic.

2. In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, a system within said mobile device for indicating the authenticity of inquiries for confidential identity codes, as described in claim 1, wherein the first and second display zones are dynamic and static displays respectively.

3. In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, a system within said mobile device for indicating the authenticity of inquiries for confidential identity codes, as described in claim 1, wherein said externally generated information is identified by said control processor.

4. In a mobile communications device adapted to communicate interactively with a remote network server, said mobile device having a control processor, a user interface and a display, a method for indicating the authenticity of inquiries for confidential identity codes comprising:

identifying said inquiries for confidential identity codes as externally generated or internally generated;

dividing said display into first and second display zones;

routing externally generated inquiries only to said first display zone; and

generating an indication symbol in said second display zone when the inquiry is internally generated, to indicate to the user that said inquiry is authentic.

5. In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, said mobile device having a control

processor, a user interface and a display, a method for indicating the authenticity of inquiries for confidential identity codes, as described in claim 4, wherein the first and second display zones are dynamic and static displays respectively.

6. In a mobile communications device adapted to communicate interactively with a remote network server, said mobile device having a control processor, a user interface and a display panel, a method for indicating the authenticity of inquiries for confidential identity codes, as described in claim 4, wherein said control processor identifies the externally generated information.

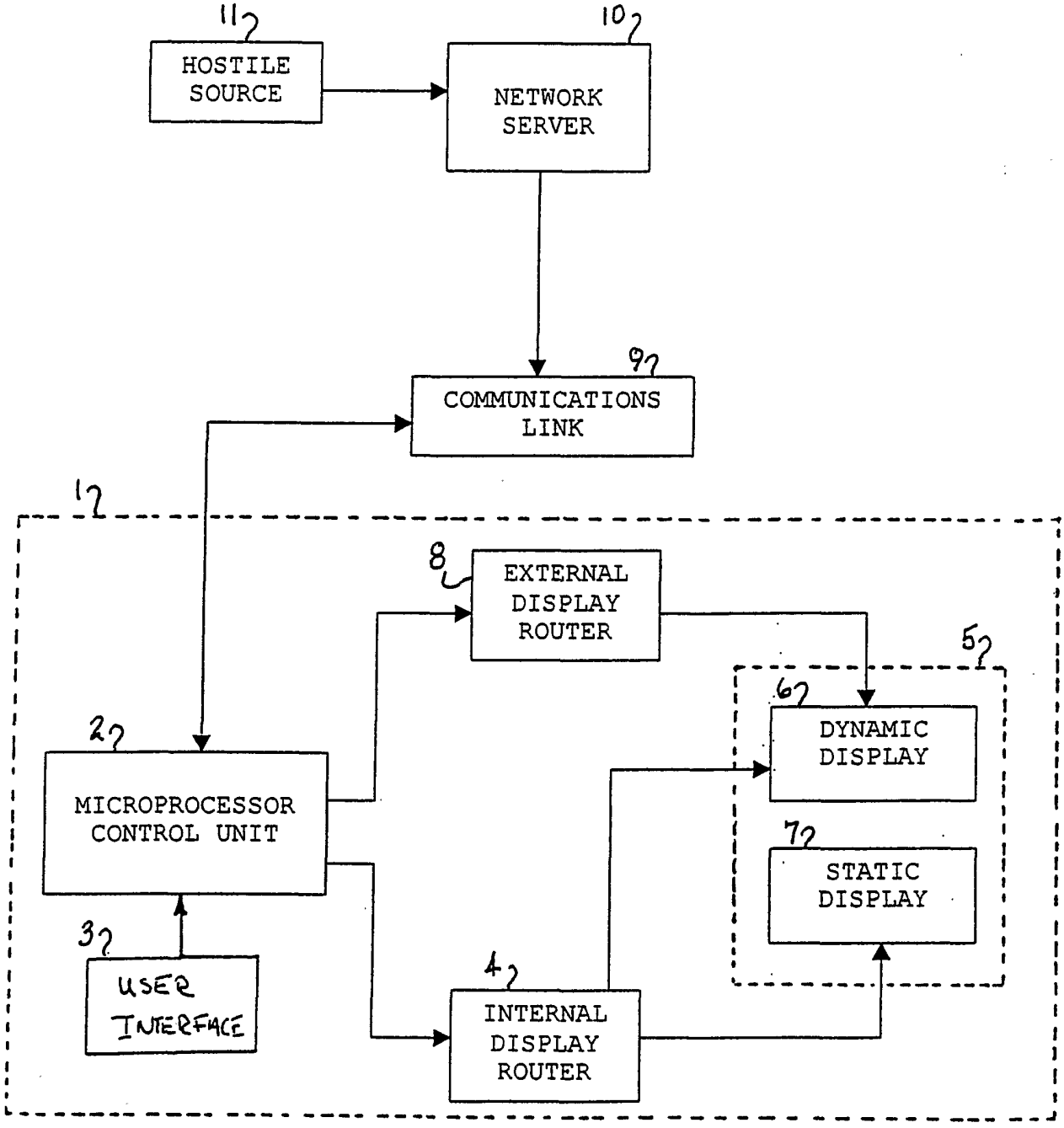
11
HOSTILE SOURCE
10
NETWORK SERVER
9
COMMUNICATIONS LINK
1
8
EXTERNAL DISPLAY ROUTER
5
6
DYNAMIC DISPLAY
7
STATIC DISPLAY
2
MICROPROCESSOR CONTROL UNIT
3
USER INTERFACE
4
INTERNAL DISPLAY ROUTER

FIGURE 1

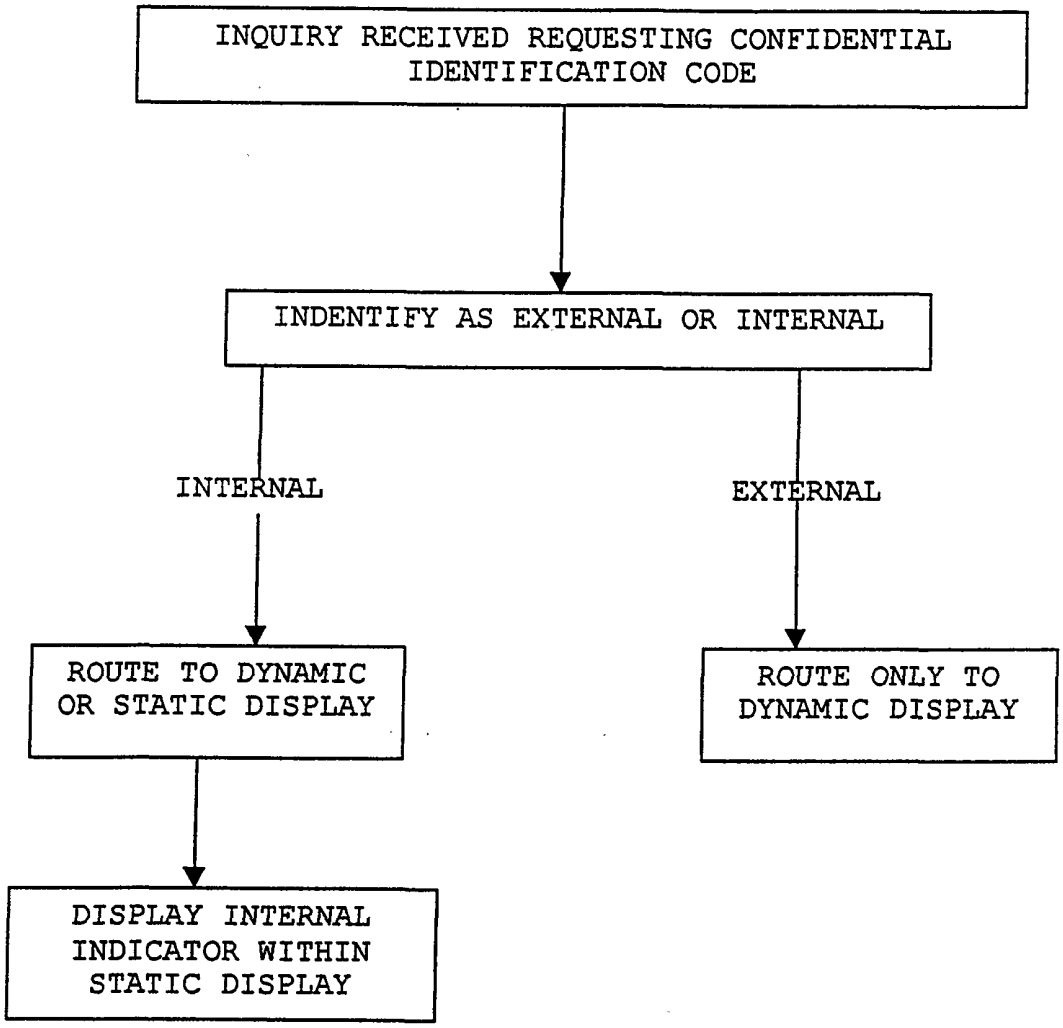
INQUIRY RECEIVED REQUESTING CONFIDENTIAL IDENTIFICATION CODE
INDENTIFY AS EXTERNAL OR INTERNAL
INTERNAL
EXTERNAL
ROUTE TO DYNAMIC OR STATIC DISPLAY
ROUTE ONLY TO DYNAMIC DISPLAY
DISPLAY INTERNAL INDICATOR WITHIN STATIC DISPLAY

FIGURE 2

Figure 3a

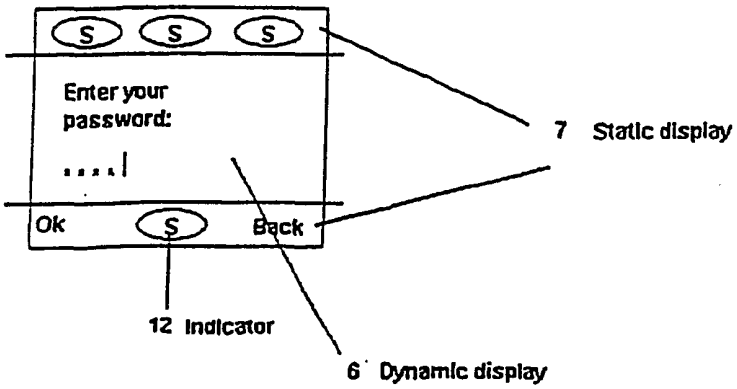


Figure 3b