(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 301 532**

(51) Int. Cl.:
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01909142 .0**
(86) Fecha de presentación : **12.02.2001**
(87) Número de publicación de la solicitud: **1264500**
(87) Fecha de publicación de la solicitud: **11.12.2002**

(54) Título: **Indicador seguro de una solicitud de acción del usuario.**

(30) Prioridad: **15.03.2000 US 525806**

(45) Fecha de publicación de la mención BOPI:
01.07.2008

(45) Fecha de la publicación del folleto de la patente:
01.07.2008

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Lukkaroinen, Mikko y**
Inget, Virve

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Indicador seguro de una solicitud de acción del usuario.

Antecedentes de la invención

A los dispositivos de comunicaciones, tales como los teléfonos móviles, los buscapersonas y otros similares, se les está dotando de cada vez más funciones. En el pasado, dicho equipos móviles han constituido un entorno cerrado, en otras palabras, todas las funciones utilizan un software situado dentro del equipo móvil o la SIM. Con la aparición de las nuevas tecnologías, las cuales utilizan protocolos de comunicaciones inalámbricas, tales como el Protocolo de Aplicación Inalámbrica (WAP) o protocolos comparables, el dispositivo móvil puede acceder a aplicaciones adicionales, desde servidores de red. Como consecuencia, surge una nueva amenaza para la seguridad de los equipos móviles. En poco tiempo, los equipos móviles se verán expuestos a cuestiones diseñadas para extraer información de seguridad confidencial del usuario, tal como un PIN u otro identificador. Por esta razón es necesario idear un sistema fiable en el cual se puedan identificar e ignorar fácilmente solicitudes de información originadas en fuentes remotas "hostiles".

El documento WO 99/59334 da a conocer un sistema de navegador personal que incluye un componente de visualización para visualizar una lista de selección con división dual. La lista de selección con división dual está adaptada para visualizar información recibida externamente y comprende una primera lista de selección y una segunda lista de selección. Se pueden visualizar simultáneamente partes de la primera y la segunda listas de selección.

El documento WO 00/01180 da a conocer un teléfono móvil que incluye unos medios de procesado para combinar datos de identidad recibidos y datos de clave recibidos con vistas a producir datos de seguridad recibidos, y medios de comparación para comparar los datos de seguridad recibidos con datos de seguridad almacenados con vistas a determinar si se va a procesar una instrucción de datos recibida.

Uno de los objetivos de la presente invención es proporcionar un sistema para identificar consultas remotas que puedan provocar una fisura de seguridad en el uso de equipos móviles tales como un teléfono móvil, un buscapersonas u otro dispositivo de comunicaciones similar.

Sumario de la invención

Para usar aplicaciones accesibles a partir de un servidor de red, se diseña un dispositivo móvil para un uso interactivo. Esta opción permite que el dispositivo móvil ejecute dichas aplicaciones almacenadas en un servidor de red remoto desde el dispositivo móvil. Para reducir el riesgo de recepción de solicitudes fraudulentas de identificadores confidenciales, se diseña un sistema para identificar consultas generadas externamente. Con este fin, se proporcionan unos medios para compartimentar la visualización de solicitudes de información remotas. El dispositivo móvil está equipado de una pantalla que está dividida en zonas de visualización dinámica y estática. Las consultas generadas externamente se pueden escribir únicamente en la zona dinámica. Las consultas generadas internamente activarán un indicador en la zona estática para informar al usuario sobre la autenticidad de la consulta. Como consecuencia, las solicitudes de información hostiles se pueden reconocer e ignorar inmediatamente.

Según uno de los aspectos de la invención, se proporciona un sistema según se especifica mediante la reivindicación 1.

Según otro de los aspectos de la invención, se proporciona un dispositivo de comunicaciones móviles según se especifica mediante la reivindicación 3.

Según otro de los aspectos de la invención, se proporciona un método según se especifica mediante la reivindicación 4.

Descripción de los dibujos

La invención se describe más detalladamente a continuación haciendo referencia a los dibujos adjuntos en los cuales:

La Figura 1 es un diagrama de bloques de un sistema de comunicaciones que utiliza la invención en cuestión;

La Figura 2 es un diagrama de flujo de información del método de la presente invención; y

Las Figuras 3a y 3b ilustran unas formas de realización de la pantalla compartimentada de la presente invención.

Descripción de la forma de realización preferida

Los componentes básicos del sistema de comunicaciones de la presente invención se muestran en el diagrama de bloques de la figura 1. Un dispositivo móvil 1 está conectado a través de un enlace de comunicaciones 9 a un servidor de red 10. En este caso, el servidor de red 10 además de facilitar el tráfico de las comunicaciones también proporciona aplicaciones interactivas tales como banca, correo electrónico, inversiones y otras funciones.

El dispositivo móvil 1 incluye una unidad de control de microprocesador (MCU) 2 a la que accede el usuario a través de una interfaz de usuario 3, tal como un teclado. La pantalla 5 comunica información desde la MCU 2 al usuario. La MCU 2 contiene el software o microprograma requerido para ejecutar las funciones sobre el dispositivo móvil 2 necesarias para hacer funcionar las aplicaciones que residen en el servidor de red 10. Muchas de las aplicaciones requerirán el uso de identificadores de seguridad, tales como números PIN y otros códigos confidenciales para acceder a los archivos de aplicación personales del usuario.

En los primeros tiempos de los ordenadores en red, se produjo una proliferación de procedimientos fraudulentos de entrada a los sistemas que generaban consultas de información confidencial para el ordenador personal. Si esta información era suministrada, la misma era robada y usada para actividades delictivas o de otro tipo no autorizadas por el usuario. En la actualidad, el riesgo de dichas fisuras de seguridad se está convirtiendo en un problema para el usuario de dispositivos móviles, especialmente los que están equipados para sacar provecho de los protocolos de comunicaciones tales como el WAP. Estos protocolos representan procedimientos de funcionamiento normalizados para la transmisión interactiva de datos usados con vistas a ejecutar una serie variada de transacciones. Aunque muchas de estas transacciones son seguras gracias a las firmas digitales requeridas, tales como los códigos PIN, es esencial que se mantenga la confidencialidad del código. Las consultas fraudulentas constituyen una amenaza significativa para la utilidad de estas aplicaciones.

El dispositivo móvil 1 de la presente invención está equipado de una pantalla 5, la cual está dividida en dos zonas discretas, una zona de visualización estática 7 y una zona de visualización dinámica 6. Un encaminador de visualización interna 4 dirige la información y las consultas generadas internamente hacia las pantallas bien estática o bien dinámica.

Tal como se muestra en las figuras 3a y 3b, la pantalla estática 7 puede presentar iconos de menú, símbolos de herramientas, indicaciones de estados, tales como el nivel de la batería, y otras referencias administrativas. La pantalla dinámica 6 está destinada a visualizar información interactiva referente a la ejecución de las actividades de una aplicación que está en marcha. La información generada dentro del dispositivo móvil se puede visualizar en las pantallas bien estática o bien dinámica.

La información transmitida hacia el dispositivo móvil 1 desde, por ejemplo, una fuente hostil 11 a través del servidor de red 10, utilizará protocolos de navegadores y será fácilmente identificable. Esta información se dirige hacia la pantalla dinámica 6 por medio de un encaminador de visualización externa 8. De esta manera, la información proveniente del servidor de red 10 se aísla con respecto a la información generada internamente del dispositivo móvil 1.

Para informar al usuario sobre la autenticidad de consultas de códigos identificadores, en la pantalla estática 7 se visualizará un símbolo identificador 12, por ejemplo, un icono parpadeante, tal como se muestra en las figuras 3a y 3b. Cuando se visualiza este símbolo, el mismo indicará al usuario que la solicitud se ha generado internamente. Como la MCU identifica la consulta externa y esta información se encamina únicamente hacia la pantalla dinámica 6, se dispone de una indicación fiable de que se puede transmitir un número PIN sin un riesgo apreciable de uso indebido.

Tal como se muestra en la figura 2, durante el funcionamiento, si desde la fuente hostil 11 se transmite un procedimiento fraudulento de entrada al sistema a través del servidor de red 10, cuando se recibe el mismo, éste es identificado por la MCU y se encamina únicamente hacia la pantalla dinámica 6. La consulta generada externamente se puede escribir únicamente en la pantalla dinámica 6. Cuando se genera una consulta mediante la ejecución de un software interno, en la pantalla estática 7 se visualiza claramente una indicación. Cuando se responde a la consulta visualizada en la pantalla dinámica 6, se avisará al usuario de que no responda a no ser que se visualice el indicador interno.

De esta manera se puede limitar la transmisión de códigos de identificación confidenciales y se puede reducir significativamente el riesgo de una interceptación no autorizada y el uso de códigos PIN y otras operaciones similares.

REIVINDICACIONES

1. Sistema para ser utilizado dentro de un dispositivo de comunicaciones móviles (1) adaptado para permitir que un usuario se comunique de forma interactiva con un servidor de red remoto (10), para indicar la autenticidad de las consultas de códigos de identidad confidenciales, comprendiendo el sistema:

un procesador de control (2) para hacer funcionar dicho dispositivo móvil (1), estando adaptado dicho procesador (2) para identificar dichas consultas de códigos de identidad confidenciales como generados externamente o generados internamente;

una pantalla (5) para presentar información a un usuario, estando dividida dicha pantalla (5) en una primera zona de visualización dinámica (6) y una segunda zona de visualización estática (7); y

unos medios de encaminamiento (8) construidos para enviar información generada externamente solo hacia dicha primera zona de visualización (6);

en el que dicho procesador de control (2) genera un símbolo de indicación (12) en dicha segunda zona de visualización (7) cuando una consulta se identifica como generada internamente, indicando de este modo al usuario que dicha consulta es auténtica.

2. Sistema según la reivindicación 1, en el que dicha información generada externamente es identificada por dicho procesador de control (2).

3. Dispositivo de comunicaciones móviles (1) adaptado para permitir que un usuario se comunique de forma interactiva con un servidor de red remoto (10), incluyendo dicho dispositivo de comunicaciones móviles (1) un sistema según la reivindicación 1 ó la reivindicación 2.

4. Método para indicar la autenticidad de una consulta de un código de identidad confidencial en un dispositivo de comunicaciones móviles (1) adaptado para comunicarse de forma interactiva con un servidor de red remoto (10), presentando dicho dispositivo móvil (1) un procesador de control (2), una interfaz de usuario (3) y una pantalla (5), comprendiendo el método:

identificar dichas consultas de códigos de identidad confidenciales como generadas externamente o generadas internamente;

dividir dicha pantalla (5) en una primera zona de visualización dinámica (6) y una segunda zona de visualización estática (7);

encaminar consultas generadas externamente solo hacia dicha primera zona de visualización (6); y

generar un símbolo de indicación en dicha segunda zona de visualización (7) cuando una consulta se identifica como generada internamente, indicando de este modo al usuario que dicha consulta es auténtica.

5. Método según la reivindicación 4, que comprende la identificación de información generada externamente con el procesador de control (2).

6. Programa de ordenador que comprende unos medios de código para controlar una unidad de control de microprocesador para realizar la totalidad de las etapas del método de la reivindicación 4 ó la reivindicación 5.

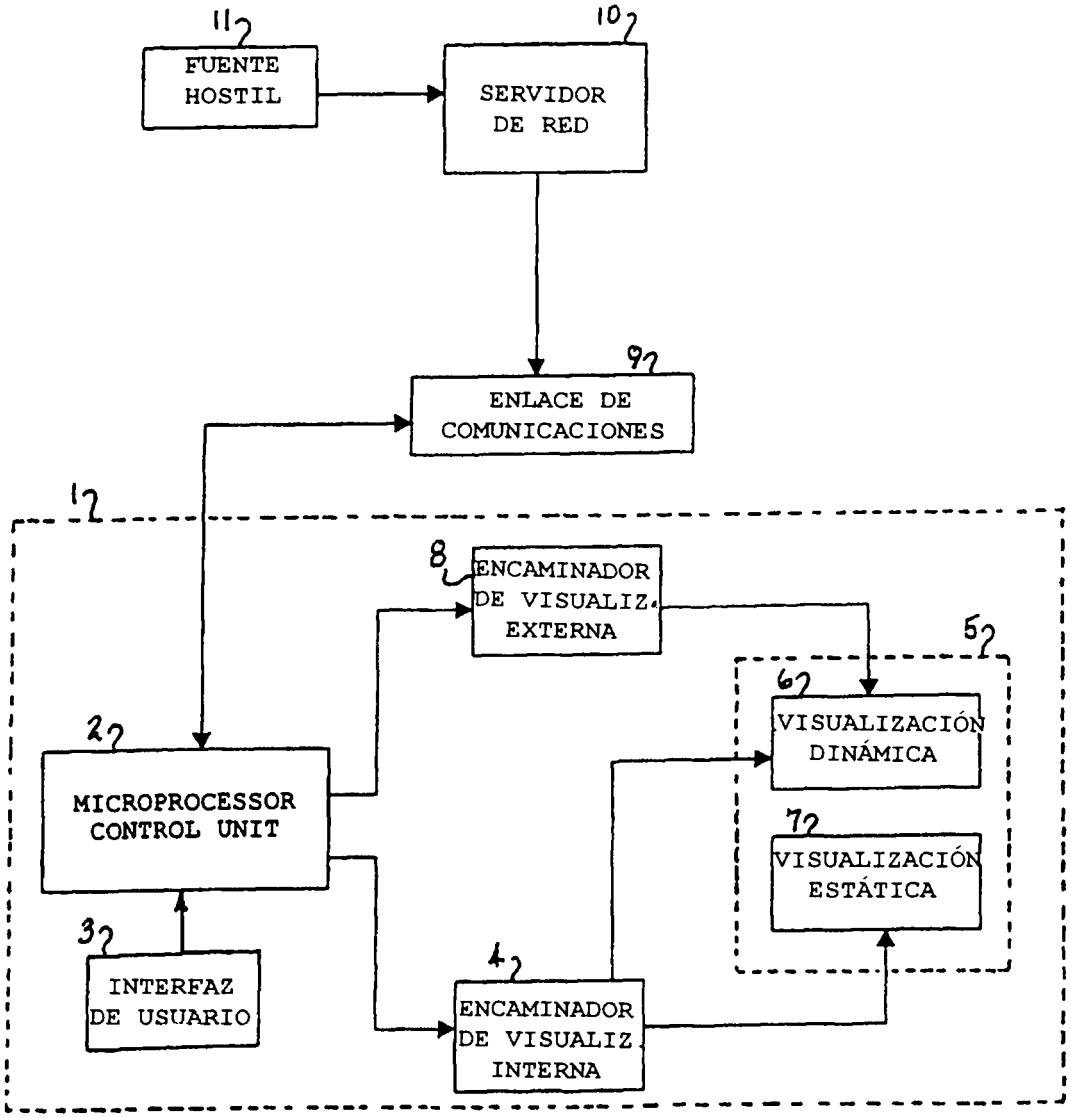
11
FUENTE HOSTIL
10
SERVIDOR DE RED
9
ENLACE DE COMUNICACIONES
1
8
ENCAMINADOR DE VISUALIZ. EXTERNA
5
6
VISUALIZACIÓN DINÁMICA
7
VISUALIZACIÓN ESTÁTICA
2
MICROPROCESSOR CONTROL UNIT
3
INTERFAZ DE USUARIO
4
ENCAMINADOR DE VISUALIZ. INTERNA

FIGURA 1

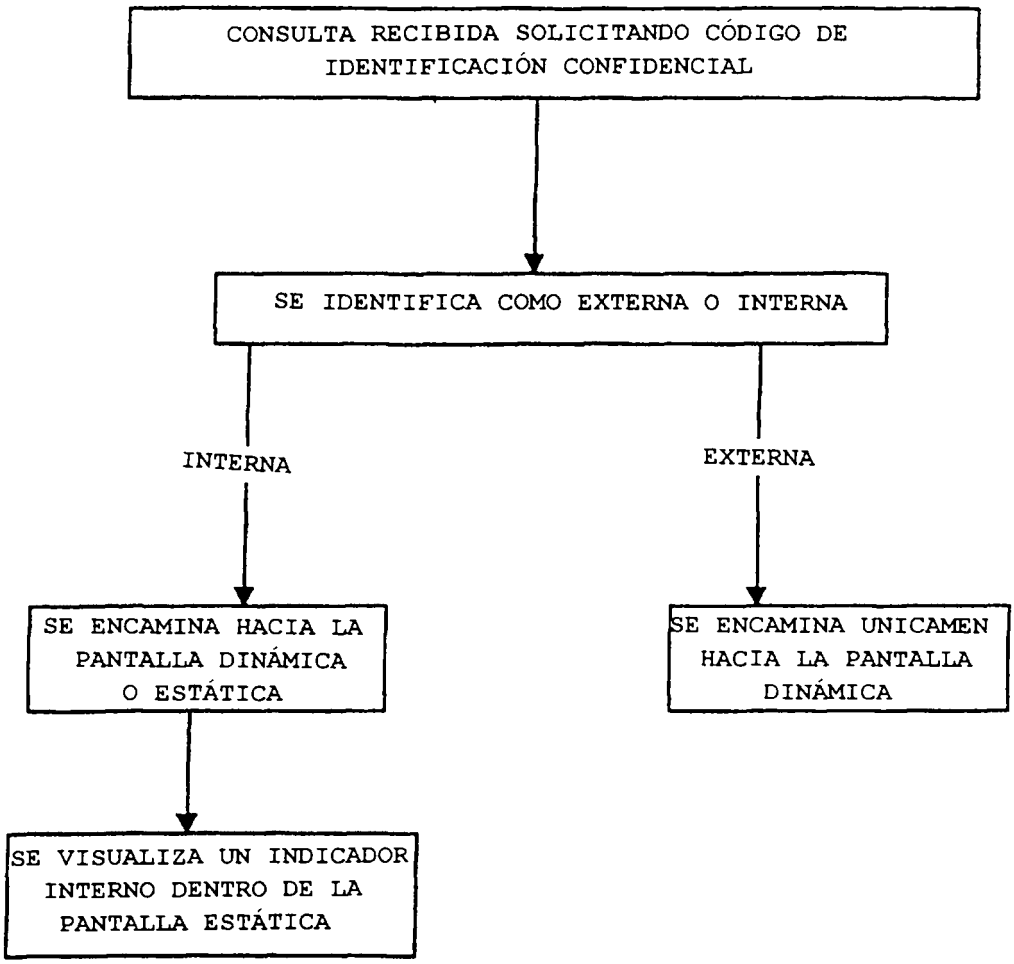
CONSULTA RECIBIDA SOLICITANDO CÓDIGO DE IDENTIFICACIÓN CONFIDENCIAL
SE IDENTIFICA COMO EXTERNA O INTERNA
INTERNA
EXTERNA
SE ENCAMINA HACIA LA PANTALLA DINÁMICA O ESTÁTICA
SE ENCAMINA UNICAMEN HACIA LA PANTALLA DINÁMICA
SE VISUALIZA UN INDICADOR INTERNO DENTRO DE LA PANTALLA ESTÁTICA

FIGURA 2

FIGURA 3a

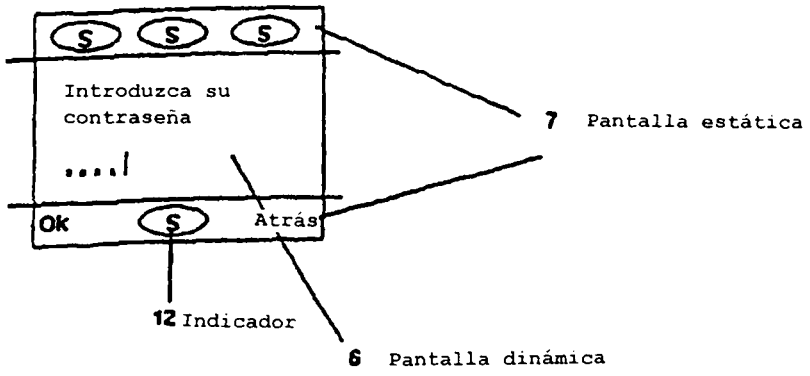

FIGURA 3b