

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
13. Februar 2003 (13.02.2003)

PCT

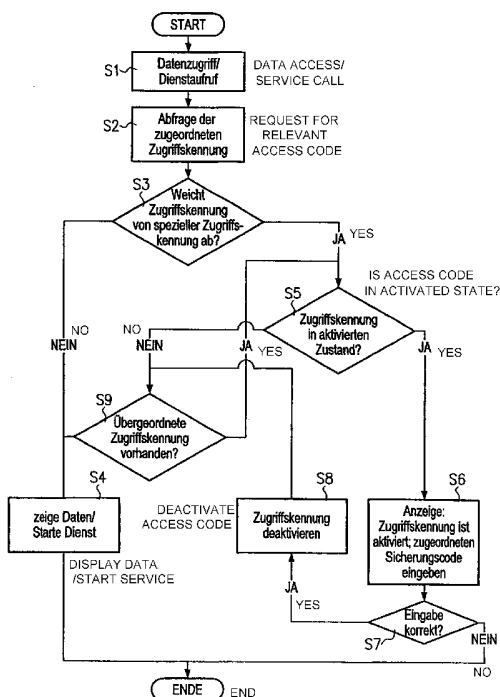
(10) Internationale Veröffentlichungsnummer  
WO 03/013170 A2

- (51) Internationale Patentklassifikation<sup>7</sup>: H04Q 7/38 (72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): WENZEL, Dietmar [DE/DE]; Am Jagdweg 2, 81549 München (DE). HAUSNER, Josef [DE/DE]; Schützenstrasse 7, 82110 Germering (DE).
- (21) Internationales Aktenzeichen: PCT/DE02/02034
- (22) Internationales Anmeldedatum: 4. Juni 2002 (04.06.2002)
- (25) Einreichungssprache: Deutsch (74) Anwalt: LAMBSDORFF, Matthias; Dingolfinger Strasse 6, 81673 München (DE).
- (26) Veröffentlichungssprache: Deutsch (81) Bestimmungsstaaten (national): CN, JP, US.
- (30) Angaben zur Priorität: 101 35 527.0 20. Juli 2001 (20.07.2001) DE (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Strasse 53, 81669 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: MOBILE STATION IN A MOBILE COMMUNICATION SYSTEM AND METHOD FOR ACCESSING A SERVICE AND/OR A DATA SET IN THE STAND-BY MODE OF THE MOBILE STATION

(54) Bezeichnung: MOBILSTATION EINES MOBILKOMMUNIKATIONSSYSTEMS UND VERFAHREN ZUM ZUGREIFEN AUF EINEN DIENST UND/ODER EINEN DATENSATZ IM BEREITSCHAFTSMODUS DER MOBILSTATION



S3 - IS ACCESS CODE DIFFERENT FROM THE PARTICULAR ACCESS CODE?  
S5 - IS ACCESS CODE IN ACTIVATED STATE?  
S6 - DISPLAY: ACCESS CODE IS ACTIVATED; INPUT RELEVANT SECURITY CODE  
S7 - INPUT CORRECT?  
S9 - IS OVERRIDING ACCESS CODE AVAILABLE?

(57) Abstract: A mobile station (1) comprising a transmission and receiving unit and an identification module (SIM), for application within the mobile station, provides a user with services and/or data sets in the stand-by mode, which can be called up by the user. According to the invention, an unauthorised access to the services and/or data sets may be avoided, whereby each service and/or data set has a characteristic access code, which may be activated or deactivated by means of the input or transmission of a security code. The mobile station (1) comprises security means (2, 3, 4, 5, 5a, 6, 9, 10, 11, 12, 13) for the input and/or transmission of the security code. Access to a service and/or data set is blocked or permitted depending on the status of the access code in the stand-by mode for the mobile station (1).

(57) Zusammenfassung: Eine Mobilstation (1) mit einer Sendeeinheit und einem, in die Mobilstation einsetzbaren Identifikationsmodul (SIM), stellt im Bereitschaftsmodus einem Nutzer Dienste und/oder Datensätze bereit, die von dem Nutzer abgerufen werden können. Um einen unberechtigten Zugriff auf die Dienste und/oder Datensätze zu vermeiden, wird jedem Dienst und/oder Datensatz eine charakteristische Zugriffskennung zugeordnet, die durch Eingeben und/oder Übertragen eines zugeordneten Sicherungscodes aktiviert oder deaktiviert wird. Zum Eingeben und/oder Übertragen des Sicherungscodes weist die Mobilstation (1) Sicherheitmittel (2, 3, 4, 5, 5a, 6, 9, 10, 11, 12, 13) auf. Abhängig vom Zustand der Zugriffskennung, ob aktiviert oder deaktiviert, ist ein Zugriff auf einen Dienst und/oder Datensatz im Bereitschaftsmodus der Mobilstation (1) gesperrt bzw. freigegeben.

WO 03/013170 A2



**Veröffentlicht:**

— ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

## Beschreibung

Mobilstation eines Mobilkommunikationssystems und Verfahren zum Zugreifen auf einen Dienst und/oder einen Datensatz im Bereitschaftsmodus der Mobilstation

Die Erfindung betrifft eine Mobilstation eines Mobilkommunikationssystems und ein Verfahren zum Zugreifen auf einen Dienst und/oder einen Datensatz im Bereitschaftsmodus der Mobilstation.

In einer Mobilstation die üblicherweise aus einem Sende- und Empfangsgerät und einem Identifikationsmodul besteht, sind meistens persönliche, benutzerbezogene Datensätze verschiedenster Datenkategorien gespeichert (zum Beispiel Telefonnummern, Adressen, Termine, Texte und Spachaufzeichnungen). Des Weiteren werden Dienste (zum Beispiel Internet, E-Mail) bereitgestellt. Im ausgeschalteten Zustand der Mobilstation sind die Datensätze und Dienste im allgemeinen vor unberechtigtem Zugriff und unberechtigter Nutzung geschützt sowie ein unberechtigter Verbindungsaufbau unterbunden, da nach dem Stand der Technik meistens eine Personal Identification Number (PIN) vom Benutzer über die Tastatur in die Mobilstation eingegeben werden muss, um die Mobilstation einzuschalten beziehungsweise deren Bereitschaftsmodus zu aktivieren. So ist es beispielsweise bei Mobiltelefonen üblich, dass nach Inbetriebnahme dieser Geräte eine in den meisten Fällen vierstellige PIN abgefragt wird, ohne deren richtige Eingabe keine Einbuchung ins Netz des Netzbetreibers erfolgt. Hierdurch wird sichergestellt, dass abgeschaltete Mobiltelefone wegen der ohne vorherigen PIN-Eingabe nicht gegebenen Benutzungsmöglichkeit, für Diebe reizlos sind.

Auch wenn diese Sicherungsfunktion bei Mobiltelefonen, die von den Benutzern nicht ständig mitgeführt werden, ihre Berechtigung hat, wird es doch zum Teil als lästig empfunden, zur Individualisierung einer befugten Nutzung die PIN einzu-

geben, um das Mobiltelefon zunächst in den Bereitschaftszu-  
stand zu bringen. Die PIN bietet daher den Schutz, dass eine  
Mobilstation entweder nur im ausgeschalteten Zustand gesi-  
chert ist oder im Bereitschaftszustand allgemein zur Verfü-  
5 gung steht. Dadurch besteht besonders dann die Gefahr einer  
unberechtigten Nutzung oder eines Diebstahls, wenn die Mobil-  
station im Bereitschaftszustand unbeaufsichtigt vom berech-  
tigten Nutzer ist.

10 Ist die Mobilstation im Bereitschaftsmodus, d.h. es kann ent-  
weder eine Verbindung zur Basisstation von der Mobilstation  
initiiert werden oder die Mobilstation ist empfangsbereit für  
eine von der Basisstation initiierte Verbindung, ist bisher  
kein personenbezogener Schutz der Daten oder Dienste, die  
15 über die Mobilstation bereitgestellt werden, möglich.

Bei einer bekannten Vorrichtung (DE 299 15 915 U1) ist der  
Zugriff auf einen Dienst und/oder einen Datensatz im Bereit-  
schaftsmodus der Mobilstation dadurch gesichert, dass die Mo-  
20 bilstation einen eingebauten Sender mit Miniempfänger auf-  
weist. Der eingebaute Sender arbeitet auf Funkbasis und be-  
einträchtigt in keiner Weise die Funktion des Mobiltelefons  
solange der Miniempfänger im Empfangsbereich liegt. Der Mi-  
niempfänger befindet sich dabei am Schlüsselbund des Mobilte-  
25 lefonbesitzers. Entfernt sich nun der Besitzer von seinem Mo-  
biltelefon um mehr als zwei bis fünf Meter, gibt der Miniemp-  
fänger sofort einen akustischen und visuellen Alarm, im glei-  
chen Moment wird die Tastatur des Mobiltelefons gesperrt.  
Kommt der Mobiltelefonbesitzer wieder in Sendereichweite,  
30 wird die Tastatur sofort entsperrt und steht wieder zur Ver-  
fügung. Um das Sicherheitssystem zu deaktivieren, wird der  
Miniempfänger abgeschaltet, dadurch wird die Tastatur zwar  
gesperrt, kann aber mittels einer Codenummer, die jedem Mo-  
biltelefon zur Verfügung steht, wieder entsperrt werden.

35

Die üblicherweise implementierte Tastatursperre, die aus dem  
Stand der Technik in bereits mehreren Ausführungsformen be-

kannt ist, stellt keine personenbezogene Schutzmöglichkeit dar, sondern lediglich einen bestenfalls gerätespezifischen Schutzmechanismus vor unbeabsichtigter Tastaturbetätigung.

5 Oftmals wird die Mobilstation längere Zeit im Bereitschaftszustand betrieben und wird an Orten aufbewahrt, die mehreren Personen zugänglich sind. Insbesondere in solchen Situationen oder wenn die Mobilstation im Bereitschaftszustand entwendet wurde, ist ein Schutz gegen Mißbrauch und unberechtigten Zugriff auf Dienste und/oder Datensätze sinnvoll.  
10

Aufgabe der Erfindung ist es, eine Mobilstation eines Mobilkommunikationssystems und ein Verfahren zum Zugreifen auf einen Dienst und/oder einen Datensatz, der einem Nutzer über  
15 die Mobilstation angeboten wird und von dem Nutzer abgerufen werden kann, zu schaffen, bei der beziehungsweise bei dem mit hoher Sicherheit eine unberechtigte Nutzung des Dienstes und/oder des Datensatzes im Bereitschaftsmodus der Mobilstation verhindert werden kann.

20

Diese Aufgabenstellung wird erfindungsgemäß durch eine Mobilstation, welche die Merkmale nach Patentanspruch 1 aufweist sowie durch ein Verfahren, dass die Schritte nach Patentanspruch 14 aufweist, gelöst.

25

Eine Mobilstation eines Mobilkommunikationssystems weist eine Sende- und Empfangseinheit zum Übertragen von elektrischen Signalen zwischen der Mobilstation und einer oder mehreren weiteren Mobilstationen über eine oder mehrere Basisstationen  
30 oder zwischen der Mobilstation und einer oder mehreren Basisstation auf. Desweiteren weist die Mobilstation ein in die Mobilstation einsetzbares Identifikationsmodul (SIM) zum Überprüfen einer Nutzungsberechtigung der Mobilstation durch einen Nutzer und zum Aktivieren des Bereitschaftsmodus der  
35 Mobilstation, welche zumindest einen Dienst und/oder Datensatz bereitstellt der von einem Nutzer abrufbar ist, auf.

Erfindungsgemäß ist dem bereitgestellten Dienst und/oder Datensatz eine charakteristische Zugriffskennung zugeordnet. Die Zugriffskennung ist dabei durch einen individuellen Sicherungscode gesichert. Die Mobilstation weist dazu ein Sicherungsmittel auf, dass zumindest im Bereitschaftsmodus der Mobilstation aktiv ist. Durch Eingabe und/oder Übertragung des Sicherungscode in beziehungsweise an das Sicherungsmittel ist die Zugriffskennung aktivierbar oder deaktivierbar. Indem die Zugriffskennung aktiviert oder deaktiviert ist, ist der Zugriff auf den Dienst und/oder den Datensatz gesperrt beziehungsweise freigegeben.

Dadurch kann erreicht werden, dass der Zugriff auf den Dienst und/oder Datensatz der über die Mobilstation bereitgestellt wird, für einen unberechtigten Nutzer verhindert wird. Die Mobilstation ist dadurch auch im Bereitschaftsmodus, wenn sie vom berechtigten Nutzer unbeaufsichtigt ist, vor unberechtigtem Zugriff gesichert.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

Es kann dabei vorgesehen sein, dass die Zugriffskennung eine oder mehrere Zahlen und/oder einen oder mehrere Buchstaben und/oder ein oder mehrere Sonderzeichen aufweist.

Dadurch kann erreicht werden, dass für die Zugriffskennung eine Vielzahl an Kombinationen von Zeichen, Buchstaben und Sonderzeichen möglich sind und somit eine erhöhte Sicherheit gegen unberechtigten Zugriff auf einen Dienst und/oder Datensatz gewährleistet ist.

Desweiteren kann vorgesehen sein, dass der Sicherungscode gleich einem PIN-Code ist, der zum Aktivieren des Bereitschaftsmodus der Mobilstation eingegeben wird. Der Sicherungscode kann aber auch so ausgeführt sein, dass der Code ein oder mehrere alphanumerische Zeichen aufweist und somit aus

zumindest einem Buchstaben oder zumindest einer Ziffer besteht. Eine weitere Ausführungsform ist dadurch gegeben, dass der Sicherungscode ein oder mehrere graphische Zeichen und/oder ein oder mehrere graphische Symbole aufweist.

5

Dadurch stehen dem Nutzer eine Vielzahl an Kombinationsmöglichkeiten für den Sicherungscode zur Verfügung und eine möglichst einfache Gestaltung des Sicherungscodes kann gewährleistet werden. Zusätzlich kann dadurch die Wahrscheinlichkeit reduziert werden, dass ein unberechtigter Nutzer den Sicherheitscode durch einfaches Ausprobieren herausfindet.

10

Neben diesen Ausführungsformen des Sicherungscodes kann als weitere Alternative ein biometrisches Merkmal eines berechtigten Nutzers der Mobilstation als Sicherungscode dienen. Als biometrisches Merkmal kann dabei beispielsweise ein Fingerabdruck herangezogen werden. Es kann aber auch das Augenbild des berechtigten Nutzers als biometrisches Kennzeichen herangezogen werden.

15

20

Der Sicherungscode kann aber auch ein akustisches Merkmal des berechtigten Nutzers, beispielsweise die gesprochene Sprache, sein.

25

Dadurch kann erreicht werden, dass der Sicherungscode durch ein individuelles Merkmal des berechtigten Nutzers charakterisiert ist. Ein weiterer Vorteil dabei ist, dass das Eingeben und Überprüfen des biometrischen Merkmals relativ schnell erfolgt und das keine Erfordernis seitens des berechtigten Nutzers besteht, sich ein oder mehrere Kombinationen aus Zeichen, Ziffern, Buchstaben und dergleichen merken zu müssen.

30

Eine weitere Möglichkeit der Ausgestaltung des Sicherungscodes ist dadurch gegeben, dass der Sicherungscode ein elektrisches Signal ist, das drahtlos an die Mobilstation übertragen wird.

35

Es kann auch vorgesehen sein, den Sicherungscode als Strichcode oder als Magnetcode, beispielsweise auf einer Chipkarte, auszuführen.

- 5    Dadurch ist ebenfalls die Möglichkeit einer relativ schnellen Eingabe oder Übertragung des Sicherungscodes an die Mobilstation, sowie eine hohe Sicherheit der Dienste und/oder Datensätze gegen unberechtigte Nutzung gegeben.
- 10   Selbstverständlich ist es auch ohne weiteres möglich, ein Sicherungscode derart zu gestalten, dass er eine beliebige Kombination aus den oben angeführten Ausführungsformen darstellt.
- 15   Abhängig von der erwünschten Absicherung eines Zugriffs auf Dienste und/oder Datensätze kann somit die Wahrscheinlichkeit eines unberechtigten Zugriffs weiter vermindert werden.

Abhängig von der Gestaltung des Sicherungscodes weist die Mobilstation entsprechende Sicherungsmittel zur Eingabe und/oder Übertragung der Sicherungscodes in beziehungsweise an die Mobilstation auf. Zur Eingabe des Sicherungscodes kann dabei vorgesehen sein, dass die Mobilstation eine Tastatur und/oder eine berührungssensitive Anzeigefläche, beispielsweise ein Touch-Screen oder ein Touch-Pad, aufweist. Desweiteren kann ein Sensor zum Detektieren der biometrischen oder

20    weitere Merkmale des berechtigten Nutzers vorgesehen sein.

- 30   Zum Übertragen des als elektrisches Signal ausgeführten Sicherungscodes kann ein tragbarer Transponder vorgesehen sein, der durch das Betätigen durch den berechtigten Nutzer das elektrische Signal aussendet, welches von einem entsprechenden Empfänger in der Mobilstation empfangen und auf seine Berechtigung hin überprüft werden kann.
- 35

Die Mobilstation kann auch eine Scannervorrichtung aufweisen, mittels der, als Strichcode oder Magnetcode auf einer Chipkarte ausgeführte Sicherungscode abgetastet wird. Die Scannervorrichtung kann dabei in der Mobilstation angeordnet sein  
5 oder durch eine elektrische Verbindung mit der Mobilstation verbunden sein.

Werden über die Mobilstation mehrere Dienste und/oder Datensätze einem Nutzer angeboten, kann vorteilhafterweise vorge-  
10 sehen sein, dass eine Zugriffskennung mehreren Diensten und/oder Datensätzen zugeordnet wird. Es ist auch möglich, dass jedem Dienst und/oder Datensatz mehrere Zugriffskennungen entsprechend einer Hierarchiestruktur zugeordnet sind. Sowohl die Zuordnung als auch die Gestaltung der Hierarchie-  
15 struktur kann dabei zumindest teilweise von einem berechtigten Nutzer individuell verändert werden.

Dadurch kann erreicht werden, dass der berechtigte Nutzer die Dienste und/oder Datensätze entsprechend seiner individuellen  
20 Prioritätenliste hinsichtlich der Wichtigkeit eines Schutzes vor unberechtigtem Zugriff der Dienste und/oder Datensätze sichern kann.

Vorteilhafterweise weist die Mobilstation einen Timer auf,  
25 der nach Ablauf einer festlegbaren Zeitdauer, innerhalb der keine Dienste und/oder Datensätze im Bereitschaftsmodus der Mobilstation von einem Nutzer abgefragt werden, Zugriffscodes automatisch aktiviert. Die automatisch zu aktivierenden Zugriffscodes können dabei ebenfalls vom berechtigten Nutzer  
30 vorab festgelegt werden.

Damit kann auch dann ein unberechtigter Zugriff verhindert werden, wenn ein berechtigter Nutzer vergisst, explizit bestimmte Dienste und/oder Datensätze im Bereitschaftsmodus der  
35 Mobilstation zu sichern.

Alle vom Benutzer eingegebenen Zugriffskennungen und zugeordneten Sicherungscodes können dabei in der Mobilstation und/oder im Identifikationsmodul (SIM) der Mobilstation gespeichert oder verschlüsselt gespeichert werden. Damit kann erreicht werden, dass eine vom berechtigten Nutzer eingestellte Zuordnung der Zugriffskennungen und Sicherungscodes so lange besteht, bis Sie vom berechtigten Nutzer verändert wird. Die Einstellungen bleiben daher auch im ausgeschalteten Zustand der Mobilstation erhalten.

10

Unabhängig davon, wie viele Dienste und/oder Datensätze, die einem Nutzer im Bereitschaftsmodus der Mobilstation bereitgestellt werden, durch aktivierte Zugriffskennungen gesperrt sind, können ankommende Verbindungen empfangen und von einem Nutzer entgegengenommen werden.

15

Ausführungsbeispiele der Erfindung werden im folgenden anhand der schematischen Zeichnungen näher erläutert. Es zeigen:

- 20 Fig. 1 einen Ablauf eines erfindungsgemäßen Verfahrens,
- Fig. 2 eine Darstellung einer Zuordnung von Diensten und/oder Datensätzen zu charakteristischen Zugriffskennungen und Sicherungscodes,
- 25 Fig. 3 ein weiteres Ausführungsbeispiel einer Zuordnung von Diensten und/oder Datensätzen zu charakteristischen Zugriffskennungen und Sicherungscodes,
- 30 Fig. 4 eine Mobilstation mit einer Tastatur und einem Display,
- Fig. 5 eine Mobilstation mit einer Scannervorrichtung,
- 35 Fig. 6 eine Mobilstation mit einem Sensor zur Detektion eines Fingerabdrucks eines Nutzers,

Fig. 7 eine Mobilstation mit einem Empfänger für elektrische Signale und einem tragbaren Transponder, und

5 Fig. 8 eine Mobilstation mit einem Sensor zur Detektion eines Augenbildes eines Nutzers und einem Sensor zur Aufzeichnung von Sprachsignalen eines Nutzers.

Ein erfindungsgemäßes Verfahren zum Zugreifen auf einen Dienst und/oder einen Datensatz, welche im Bereitschaftsmodus  
10 einer Mobilstation einem Nutzer bereitgestellt werden, wird dadurch gestartet, dass von einem Nutzer der Mobilstation versucht wird, einen Dienst und/oder einen Datensatz gemäß Verfahrensschritt S1 abzurufen (Fig. 1). Unter dem Bereit-  
15 schäftsmodus der Mobilstation wird dabei der Betriebszustand verstanden, den die Mobilstation einnimmt, wenn eine korrekte Identifizierung des Nutzers, beispielsweise durch Eingabe einer Personal Identification Number (PIN) erfolgt ist und die Dienste und/oder Datensätze über die Mobilstation bereitgestellt werden.

20

Indem der Nutzer versucht einen Dienst und/oder Datensatz zu starten oder abzufragen, wird vor der Freigabe des Zugriffs eine diesem Dienst und/oder diesem Datensatz zugeordnete charakteristische Zugriffskennung gemäß Verfahrensschritt S2 ab-  
25 gefragt. Das Zuordnen der charakteristischen Zugriffskennung zu dem Dienst und/oder Datensatz wird dabei durch den berechtigten Nutzer durchgeführt. Eine einzige Zugriffskennung kann auch mehreren unterschiedlichen Diensten und/oder Datensätzen zugeordnet werden, wodurch eine Gruppenbildung möglich ist.

30 Das Zuordnen kann zu beliebigen Zeitpunkten während des Bereitschaftsmodus der Mobilstation durchgeführt werden und wird in einem Identifikationsmodul (SIM) und/oder in der Mobilstation gespeichert. Eine durch einen berechtigten Nutzer eingestellte Zuordnung der charakteristischen Zugriffskennun-  
35 gen zu den Diensten und/oder Datensätzen bleibt auch im abgeschalteten Zustand der Mobilstation gespeichert und wird erst durch eine neue Zuordnung der Zugriffskennungen zu den Dien-

sten und/oder Datensätzen durch den berechtigten Nutzer verändert.

Beim Abfragen der Zugriffskennung wird zunächst überprüft, ob  
5 die zugeordnete charakteristische Zugriffskennung einer speziellen Zugriffskennung gemäß Verfahrensschritt S3 entspricht. Diese spezielle Zugriffskennung wird vorab durch Eingabe in die Mobilstation durch einen berechtigten Nutzer allen denjenigen Diensten und/oder Datensätzen zugeordnet,  
10 deren Inhalt oder deren Nutzung auch einem unberechtigten Nutzer zugänglich sein kann. Diese spezielle Zugriffskennung wird dabei weder in einen aktivierten noch in einen deaktivierten Zustand gesetzt. Daher wird der speziellen Zugriffskennung auch kein individueller Sicherungscode zugeordnet,  
15 mit dem ein Aktivieren oder Deaktivieren der speziellen Zugriffskennung durchgeführt wird.

Wird erkannt, dass dem Dienst und/oder Datensatz diese spezielle Zugriffskennung zugeordnet ist, so wird der Dienst  
20 und/oder der Datensatz ohne weitere Sicherheitsprüfung unmittelbar für den Nutzer gemäß Verfahrensschritt S4 zugänglich.

Wird jedoch eine von der speziellen Zugriffskennung abweichende Zugriffskennung erkannt, so wird nachfolgend überprüft, in welchem Zustand, ob im aktivierten oder deaktivierten,  
25 sich diese Zugriffskennung befindet (Verfahrensschritt S5). Bis auf die spezielle Zugriffskennung werden alle, den jeweiligen Diensten und/oder Datensätzen zugeordneten charakteristischen Zugriffskennungen entweder in den aktivierten  
30 oder den deaktivierten Zustand gesetzt.

Befindet sich die charakteristische Zugriffskennung im aktivierten Zustand, so wird ein Zugriff auf den Dienst und/oder Datensatz verhindert. Ein Nutzer wird gemäß Verfahrensschritt  
35 S6 aufgefordert, einen Sicherungscode in die Mobilstation einzugeben oder an die Mobilstation zu übertragen. Dieser Sicherungscode ist dabei speziell dieser charakteristischen Zu-

griffskennung zugeordnet. Erst wenn der dieser Zugriffskennung zugeordnete Sicherungscode korrekt in die Mobilstation eingegeben beziehungsweise an die Mobilstation übertragen wird, wird die Zugriffskennung deaktiviert. Wird ein falscher  
5 Sicherungscode gemäß Verfahrensschritt S7 eingegeben, wird ein Überprüfen des Sicherungscodes abgebrochen und ein Zugriff auf den entsprechenden Dienst und/oder Datensatz verhindert.

10 Es kann vorgesehen sein, dass bei falschem oder unkorrektem Eingeben ein Nutzer erneut aufgefordert wird, den korrekten Sicherungscode einzugeben und erst bei zwei- oder mehrmaliger unkorrekter Eingabe und/oder Übertragung ein Abbrechen des Überprüfens des Sicherungscodes erfolgt.

15

Ist der Sicherungscode korrekt in die Mobilstation eingegeben oder an die Mobilstation übertragen, so wird die charakteristische Zugriffskennung gemäß Verfahrensschritt S8 deaktiviert und der Zugriff auf den Dienst und/oder Datensatz freigegeben.  
20

Gemäß Verfahrensschritt S9 in Fig. 1 kann desweiteren vorgesehen sein, dass nach Deaktivieren der charakteristischen Zugriffskennung eine weitere Überprüfung dahingehend durchgeführt wird, ob eine weitere, dem Dienst und/oder Datensatz zugeordnete Zugriffskennung vorhanden ist und diese der ersten, bereits deaktivierten Zugriffskennung übergeordnet ist.  
25

Wird keine weitere Zugriffskennung erkannt, dann wird der Zugriff auf den Dienst und/oder Datensatz, der bereits der deaktivierten Zugriffskennung zugeordnet ist, gemäß Verfahrensschritt S4 freigegeben. Ist jedoch eine weitere Zugriffskennung vorhanden, die der ersten bereits deaktivierten Zugriffskennung übergeordnet ist, dann wird gemäß Verfahrensschritt S5 wiederum überprüft, ob diese übergeordnete Zugriffskennung aktiviert oder deaktiviert ist. Nachfolgende  
30  
35

Schritte werden dann analog zu dem bereits ausgeführten Verfahrensschritten durchgeführt.

Die Zuordnung von mehreren Zugriffskennungen zu einem Dienst und/oder Datensatz entsprechend einer Hierarchiestruktur unterliegt in der Anzahl keiner Beschränkung.

In Fig. 2 ist nachfolgend eine Tabelle eines ersten Ausführungsbeispiels einer Zuordnung von Zugriffskennungen und Sicherungscodes zu entsprechenden Diensten und/oder Datensätzen ausgeführt. Als Dienste werden dabei beispielsweise Internet und E-Mail bereitgestellt. Datensätze werden beispielsweise in Form einer privaten sowie einer dienstlichen Telefonnummernliste, einer Adressenliste und einem Jahreskalender dem berechtigten Nutzer bereitgestellt. Möchte ein Nutzer im Bereitschaftsmodus der Mobilstation den Datensatz des Jahreskalenders abrufen, so wird zunächst überprüft ob diesem Datensatz die spezielle Zugriffskennung zugeordnet ist. Die spezielle Zugriffskennung ist im Ausführungsbeispiel mit der Ziffer 0 ausgeführt. Es wird nun erkannt, dass dem Datensatz des Jahreskalenders die 0 als Zugriffskennung zugeordnet ist.

Dadurch ist der Jahreskalender jedem Nutzer freigegeben und kann von jedem Nutzer, auch von einem unberechtigten Nutzer abgerufen werden. Da die spezielle Zugriffskennungen keinen aktivierten oder deaktivierten Zustand aufweist, ist auch kein individueller Sicherungscode zugeordnet mittels den die spezielle Zugriffskennung aktiviert oder deaktiviert werden könnte. Desweiteren ist der Zugriffskennung 0 keine weitere Zugriffskennung übergeordnet, deren Zustand abgefragt werden müsste. Daher ist der Jahreskalender im Bereitschaftsmodus der Mobilstation von jedem Nutzer sofort zugänglich und kann abgerufen werden. Möchte ein Nutzer weiterhin auf den Datensatz der privaten Telefonnummern zugreifen, so wird zunächst die diesem Datensatz zugeordnete Zugriffskennung 1 erkannt. Da diese Zugriffskennung von der speziellen Zugriffskennung 0 abweicht, wird der Zustand der Zugriffskennung 1 überprüft.

Im Ausführungsbeispiel weist die Zugriffskennung 1 den aktivierten Zustand auf. Der Nutzer wird nun aufgefordert, den zugeordneten individuellen Sicherungscode 01, beispielsweise über eine Tastatur oder eine berührungssensitive Anzeigefläche einzugeben. Bei korrekter Eingabe wird die Zugriffskennung 1 in den deaktivierten Zustand gesetzt. Nachfolgend wird überprüft, ob der Zugriffskennung 1 eine weitere Zugriffskennung übergeordnet ist. Es wird dabei erkannt, dass sowohl die Zugriffskennung 3 als auch die Zugriffskennung 4 der Zugriffskennung 1 übergeordnet sind. Es wird nun überprüft, welchen Zustand die Zugriffskennungen 3 und 4 aufweisen. Sowohl die Zugriffskennung 3 als auch die Zugriffskennung 4 sind im aktivierten Zustand. Wiederum wird der Nutzer aufgefordert, die jeweils zugeordneten Sicherungscodes einzugeben. Durch die Eingabe des Sicherungscodes 2134 wird die Zugriffskennung 3 deaktiviert und durch die Eingabe des Sicherungscodes 225 wird die Zugriffskennung 4 deaktiviert. Unter der Voraussetzung der korrekten Eingabe der beiden Sicherungscodes für die Zugriffskennungen 3 und 4 wird nun der Zugriff auf den Datensatz der privaten Telefonnummern freigegeben.

Möchte ein Nutzer auf den Datensatz der dienstlichen Telefonnummern zugreifen, so wird zunächst die zugeordnete Zugriffskennung 2 erkannt. Diese Zugriffskennung 2 ist im deaktivierten Zustand, so dass der Nutzer keine Aufforderung erhält, den zugesicherten Sicherungscode 11 einzugeben, da kein Deaktivieren der Zugriffskennung 2 notwendig ist. Allerdings sind wiederum wie beim Datensatz der privaten Telefonnummern die Zugriffskennungen 3 und 4 übergeordnet. Ebenso wie beim Datensatz der privaten Telefonnummern müssen nun erst diese beiden Zugriffskennungen 3 und 4 deaktiviert werden, um einen Zugriff auf den Datensatz der dienstlichen Telefonnummern freizugeben. Gemäß der dargestellten Zuordnungstabelle muss für den Zugriff auf die Adressenliste die zugeordnete Zugriffskennung 3 deaktiviert werden. Dazu muss der zugeordnete Sicherungscode 2134 eingegeben werden.

Der Zugriffskennung 3 ist im Ausführungsbeispiel keine weitere Zugriffskennung zugeordnet. Für den Zugriff auf den E-Mail-Dienst wird die zugeordnete Zugriffskennung 4 durch  
5 Eingabe des zugeordneten Sicherungscodes 225 deaktiviert. Da der Zugriffskennung 4 die Zugriffskennung 3 übergeordnet ist und diese ebenfalls aktiviert ist, muss ebenfalls die Zugriffskennung 3 durch Eingabe des Sicherungscodes 2134 in die Mobilstation deaktiviert werden, um den Zugriff auf den E-  
10 Mail-Dienst freizugeben. Der Zugriff auf den Internetdienst ist im Ausführungsbeispiel sofort möglich. Die zugeordnete Zugriffskennung 5 ist deaktiviert und desweiteren ist ihr keine weitere Zugriffskennung übergeordnet.

15 In diesem Ausführungsbeispiel wurden sowohl die charakteristischen Zugriffskennungen als auch die übergeordneten Zugriffskennungen als auch die individuellen Sicherungscodes als Ziffern oder Ziffernkombinationen ausgeführt. Es kann auch vorgesehen sein, dass die charakteristischen Zugriffskennungen, die übergeordneten Zugriffskennungen und auch die  
20 Sicherungscodes ausschließlich als Sonderzeichen oder Sonderzeichenkombinationen oder ausschließlich durch Buchstaben oder Buchstabenkombinationen oder ausschließlich durch graphische Zeichen und/oder Symbole oder durch Kombinationen von  
25 graphischen Zeichen und/oder Symbolen ausgeführt sind.

Ein weiteres Ausführungsbeispiel einer Zuordnung von Zugriffskennungen und Sicherungskennungen zu Diensten und/oder Datensätzen ist in der Tabelle gemäß Fig. 3 dargestellt. Als  
30 Dienste und/oder Datensätze werden hier beispielsweise eine Liste mit privaten Telefonnummern, eine Liste mit dienstlichen Telefonnummern, eine Liste mit wichtigen dienstlichen Telefonnummern, eine Adressenliste, ein Datensatz, der alle vorab genannten Listen zusammenfasst, eine Terminliste, einen  
35 E-Mail-Dienst, einen SMS (Short Message Service)-Dienst, einen Sprachaufzeichnungsdienst, einen Bildaufzeichnungsdienst, ei-

nen Internetdienst sowie Spiele über die Mobilstation bereitgestellt.

Die Zugriffskennungen sind wiederum als Ziffern ausgeführt  
5 und den jeweiligen Diensten und/oder Datensätzen zugeordnet.  
Versucht ein Nutzer auf die Liste der privaten Telefonnummern  
zuzugreifen, wird erkannt, dass eine von der speziellen Zu-  
griffskennung 0 abweichende Zugriffskennung 1 zugeordnet ist.  
Diese ist aktiviert und der Nutzer wird aufgefordert, den zu-  
10 geordneten Sicherheitscode 1815 über die Tastatur und/oder die  
berührungssensitive Anzeigefläche einzugeben. Nach korrekter  
Eingabe wird die Zugriffskennung 1 deaktiviert und es wird  
überprüft ob, und falls ja, welche Zugriffskennungen der Zu-  
griffskennung 1 übergeordnet sind. Es wird dabei erkannt,  
15 dass die Zugriffskennungen 3 und 4 der Zugriffskennung 1  
übergeordnet sind. Daher wird nachfolgend der Zustand dieser  
beiden Zugriffskennungen 3 und 4 überprüft und festgestellt,  
dass beide Zugriffskennungen aktiviert sind. Wiederum erfolgt  
eine Aufforderung an den Nutzer die individuellen Sicherung-  
20 scodes, die diesen Zugriffskennungen 3 und 4 jeweils zugeord-  
net sind, einzugeben. Der Sicherheitscode der der Zugriffskenn-  
nung 3 zugeordnet ist, ist dabei als Ziffer und Buchstaben-  
kombination A7 ausgeführt und wird über die Tastatur und/oder  
die berührungssensitive Anzeigefläche eingegeben. Die Zu-  
25 griffskennung vier ist durch ein graphisches Symbol gesi-  
chert, das ebenfalls durch die Tastatur oder die berührungs-  
sensitive Anzeigefläche in die Mobilstation eingegeben wird.  
Das graphische Symbol kann auch als Schriftzug ausgeführt  
sein, beispielsweise eine Unterschrift des berechtigten Nut-  
30 zers oder ein Polygonzug, der mittels eines Stiftes auf die  
berührungssensitive Anzeigefläche geschrieben wird. Sind nun  
die Sicherheitscodes der Zugriffskennungen 3 und 4 korrekt  
eingegeben, so werden diese beiden Zugriffskennungen 3 und 4  
deaktiviert und der Zugriff auf die private Telefonnummernli-  
35 ste wird freigegeben.

Beim Zugreifen auf den Datensatz der dienstlichen Telefonnummernliste wird erkannt, dass die Zugriffskennung 2 zugeordnet ist und diese im deaktivierten Zustand ist. Ein Deaktivieren durch Eingabe des Sicherungscodes 53 ist daher nicht erforderlich. Allerdings sind auf der Zugriffskennung 2 die Zugriffskennungen 3 und 4 übergeordnet, so dass auch hier wiederum die beiden Zugriffskennungen 3 und 4 durch Eingeben der zugehörigen Sicherungscodes deaktiviert werden müssen, damit der Zugriff auf den Datensatz der dienstlichen Telefonnummern freigegeben wird. Zusätzlich ist im Ausführungsbeispiel dem Datensatz der wichtigen dienstlichen Telefonnummern ebenfalls die Zugriffskennung 2 zugeordnet. Möchte ein Nutzer auf diesen Datensatz zugreifen, muss, wie aus der Tabelle in Figur 3 ersichtlich, die übergeordnete Zugriffskennung 4 deaktiviert werden, indem das graphische Symbol eingegeben wird. Ebenso erfolgt beim Zugreifen auf den Datensatz der Adressenliste ein Überprüfen der Zugriffskennung. Die zugeordnete Zugriffskennung 3 wird erkannt und durch korrekte Eingabe des zugeordneten Sicherungscodes A7 deaktiviert. Dadurch ist der Zugriff auf den Datensatz der Adressenliste freigegeben.

Greift ein Benutzer auf die in der Tabelle mit Datensatz 1 bezeichneten Daten zu, so wird zunächst die zugeordnete Zugriffskennung 4 im aktivierten Zustand erkannt. Durch Eingabe des zugeordneten Sicherungscodes, der als graphisches Symbol ausgeführt ist, wird der Zugriff auf den Datensatz freigegeben. Da unter dem Datensatz 1 die Datensätze der privaten Telefonnummern, der dienstlichen Telefonnummern, der wichtigen dienstlichen Telefonnummern, die Adressenliste sowie die Terminliste zusammengefasst sind, wird auch automatisch ein Zugreifen auf diese Datensätze möglich, so lange die diesen Datensätzen zugeordneten Zugriffskennungen deaktiviert sind. Im Ausführungsbeispiel wird mit dem Freigeben des Zugriffs auf den Datensatz 1 lediglich der Zugriff auf den Datensatz der wichtigen dienstlichen Telefonnummernliste freigegeben. Denn nur dieser Datensatz weist eine zugeordnete Zugriffskennung, nämlich die Zugriffskennung 2 auf, die deaktiviert ist.

Alle anderen Datensätze, die im Datensatz 1 zusammengefasst sind, weisen eine weitere übergeordnete Zugriffskennung auf, die aktiviert ist (dienstliche Telefonnummernliste mit aktivierter übergeordneter Zugriffskennung 3, private Telefonnummernliste mit aktivierter übergeordneter Zugriffskennung 3) oder weisen eine dem Datensatz zugeordnete Zugriffskennung auf, die aktiviert ist (private Telefonnummernliste mit aktivierter Zugriffskennung 1, Adressenliste mit aktivierter Zugriffskennung 3, Termine mit aktivierter Zugriffskennung 5).

Beim Zugreifen des Nutzers auf den Datensatz Termine wird erkannt, dass die zugeordnete Zugriffskennung 5 aktiviert ist. Durch Eingeben des Sicherungscodes 24 wird diese Zugriffskennung 5 deaktiviert und der Zugriff auf den Datensatz Termine wird erst dann freigegeben, wenn auch noch die Zugriffskennung 4 für den Datensatz 1 deaktiviert wird.

Möchte ein Nutzer den E-Mail-Dienst nutzen, so wird die zugeordnete Zugriffskennung 6 überprüft und der aktivierte Zustand dieser Zugriffskennung 6 erkannt. Nachdem der Nutzer aufgefordert wird, den zugeordneten Sicherungscode einzugeben und der Nutzer die Kombination ?5? korrekt eingibt, wird dies weiter überprüft, welche Zugriffskennungen dieser Zugriffskennung 6 übergeordnet sind. Dabei wird erkannt, dass als übergeordnete Zugriffskennung die Zugriffskennung 7 zugeordnet ist. Diese ist dem SMS-Dienst zugeordnet und weist den aktivierten Zustand auf. Dieser Zugriffskennung 7 ist als Sicherungscode ein elektrisches Signal zugeordnet, das drahtlos von einem tragbaren Transponder an einen Empfänger der Mobilstation übertragen wird. Durch Betätigen des Transponders wird das elektrische Signal an den Empfänger übertragen. Wird das Signal korrekt empfangen, wird die Zugriffskennung 7 deaktiviert und der Nutzer kann auf den E-Mail-Dienst zugreifen. Zugleich kann der Nutzer nun auch auf den SMS-Dienst zugreifen, denn der Zugriffskennung 7, die dem SMS-Dienst als

charakteristische Zugriffskennung zugeordnet ist, ist keine weitere Zugriffskennung übergeordnet.

5 Beim Nutzen des Sprachaufzeichnungsdienstes durch den Nutzer wird wiederum, wie bei allen anderen anfänglichen Überprüfungen zunächst eine Überprüfung dahingehend durchgeführt, ob dem Dienst die spezielle Zugriffskennung zugeordnet ist. Auch beim Sprachaufzeichnungsdienst wird im Ausführungsbeispiel keine Zuordnung der speziellen Zugriffskennung 0 vorgenommen.

10 Dem Sprachaufzeichnungsdienst wird die Zugriffskennung 8 zugeordnet, die im aktivierten Zustand erkannt wird. Durch Abtasten eines Strichcodes, mittels einer Scannervorrichtung wird die Zugriffskennung 8 deaktiviert. Es kann dabei vorge-

15 sehen sein, dass die Scannervorrichtung in der Mobilstation angeordnet ist oder extern angeordnet ist und mittels einer elektrischen Verbindung mit der Mobilstation verbunden ist. Wird der Strichcode als richtig erkannt, wird die Zugriffskennung 8 deaktiviert. Durch Übertragen des elektrischen Signals mittels des Transponders an einen Empfänger, der in der

20 Mobilstation angeordnet ist, kann die, der Zugriffskennung 8 übergeordnete Zugriffskennung 7 deaktiviert werden und der Nutzer kann den nun freigegebenen Sprachaufzeichnungsdienst nutzen.

25 Dem Bildaufzeichnungsdienst ist die charakteristische Zugriffskennung 9 zugeordnet, die sich ebenfalls im aktivierten Zustand befindet. Durch Eingabe des Wortes "BILD" über die Tastatur oder die berührungssensitive Anzeigefläche, wird die Zugriffskennung 9 deaktiviert. Des Weiteren sind die der Zugriffskennung 9 übergeordneten Zugriffskennungen 7 und 8 entsprechend der bereits oben geschilderten Vorgehensweise zu

30 deaktivieren. Wird das Deaktivieren der Zugriffskennungen 9, 7 und 8 korrekt ausgeführt, wird der Zugriff auf den Bildaufzeichnungsdienst freigegeben.

35

Möchte ein Nutzer einen Zugang zum Internet aufbauen, so wird zunächst die diesem Dienst zugeordnete Zugriffskennung 10 er-

kannt. Die im aktivierten Zustand befindliche Zugriffskennung 10 ist durch das biometrische Kennzeichen des Fingerabdrucks des berechtigten Nutzers gesichert. Indem der Nutzer die Finger auf die dafür vorgesehene Auflagefläche eines Fingerabdrucksensors legt, wird dieser Fingerabdruck überprüft und bei Berechtigung die Zugriffskennung 10 deaktiviert. Der Nutzer kann auf den Internetdienst zugreifen.

Als letzter Dienst wird dem Nutzer im Ausführungsbeispiel die Möglichkeit, Spiele zu nutzen, bereitgestellt. Die zugeordnete, charakteristische Zugriffskennung 11 ist im aktivierten Zustand und kann durch eine Spracheingabe des berechtigten Nutzers beispielsweise das Wort "Spiele", deaktiviert werden. Als Sicherungscode kann dabei das Wort selbst und/oder ein charakteristisches akustisches Merkmal der Stimme des berechtigten Nutzers mittels eines Sensors deaktiviert werden. Bei nachgewiesener Berechtigung wird die Zugriffskennung 11 deaktiviert und der Zugriff auf die Spiele freigegeben.

Es ist auch im zweiten Ausführungsbeispiel möglich, die jeweilige Zugriffskennung als Kombination von Sonderzeichen und/oder Buchstaben und/oder graphischen Zeichen und/oder Symbolen und/oder Ziffern zu kombinieren.

In beiden Ausführungsbeispielen wurde für die spezielle Zugriffskennung die Ziffer 0 gewählt. Es kann aber auch jede andere Ziffer oder Kombination von Ziffern und/oder Buchstaben und/oder Sonderzeichen und/oder graphischen Zeichen und/oder Symbolen für die spezielle Zugriffskennung vorgesehen sein.

Ebenso ist es möglich, dass allen Diensten und/oder Datensätzen eine übergeordnete Zugriffskennung zugeordnet wird und durch Deaktivieren dieser übergeordneten Zugriffskennung ein Zugriff auf alle bereitgestellten Dienste und/oder Datensätze möglich ist. Dies ist allerdings nur dann möglich, wenn die den jeweiligen Diensten und/oder Datensätzen individuell zu-

geordneten, charakteristischen Zugriffskennungen deaktiviert sind.

5 In Fig. 4 ist eine Mobilstation 1 dargestellt, die eine Tastatur 2 sowie berührungssensitive Anzeigeflächen 3, 4, 5 und 5a aufweist. Durch das manuelle Betätigen der Tasten der Tastatur 2 und/oder der berührungssensitiven Anzeigeflächen 3, 4, 5 und 5a mittels eines Fingers oder eines Stiftes kann der entsprechende Sicherungscode eingegeben werden.

10

In Fig. 5 ist ein weiteres Ausführungsbeispiel der Mobilstation 1 dargestellt. Die Mobilstation 1 weist dabei zusätzlich eine Scannervorrichtung 6 auf. Dadurch kann ein Strichcode oder ein Magnetcode auf einer Chipkarte 7 abgetastet werden, wenn ein Nutzer die Chipkarte durch die Führung 8 und 8' der Scannervorrichtung 6 sieht. Die Scannervorrichtung 6 ist im Ausführungsbeispiel an der Längsseite der Mobilstation 1 angeordnet, kann aber auch auf der kurzen Seite der Mobilstation 1 oder an anderer Stelle angeordnet sein. Die Mobilstation 20 1 kann auch derart ausgeführt sein, dass sie nur die Scannervorrichtung 6 und keine Tastatur 2 und/oder keine berührungssensitiven Anzeigeflächen 3, 4, 5 und 5a aufweist.

In Fig. 6 ist eine Mobilstation 1 gemäß Fig. 1 dargestellt, die zusätzlich einen Fingerabdrucksensor 9 aufweist. Der Fingerabdrucksensor 9 kann dabei an der Rückseite oder aber auch an der Vorderseite oder aber an den Schmalseiten der Mobilstation 1 angeordnet sein. Ebenso kann auch hier vorgesehen sein, dass die Mobilstation 1 lediglich mit dem Fingerabdrucksensor 9 und ohne die Tastatur 2 und/oder die berührungssensitiven Anzeigeflächen 3, 4, 5 und 5a ausgeführt ist. 30

Ein weiteres Ausführungsbeispiel der Mobilstation 1 ist in Fig. 7 dargestellt. Diese Mobilstation 1 weist einen Empfänger 10 auf, mit dem drahtlos übertragene elektrische Signale von einem tragbaren Transponder 11 empfangen werden können. 35

Des weiteren weist die in Fig. 8 dargestellte Mobilstation 1 zusätzlich zur Tastatur 2 und den berührungssensitiven Anzeigeflächen 3, 4, 5 und 5a einen Sensor 12 auf, mit dem Sprachsignale, die von einem Nutzer gesprochen werden, detektiert werden. Zusätzlich weist die Mobilstation 1 auch einen zweiten Sensor 13 auf, mit dem das Augenbild des Nutzers detektiert werden kann und der beispielsweise an der Rückseite der Mobilstation 1 angeordnet ist.

Bei allen Ausführungsbeispielen der Mobilstation 1 in den Fig. 4 bis 8 ist es möglich, dass die Mobilstation 1 sowohl jeweils nur ein Mittel zur Eingabe und/oder Übertragung des Sicherungscodes aufweist oder aber eine beliebige Kombination der dargestellten Mittel zur Eingabe und/oder Übertragung des Sicherungscodes aufweist.

Unter einer Mobilstation wird beispielsweise ein Mobiltelefon, ein Autotelefon, ein Satellitentelefon oder ein Satellitenfax verstanden.

Die aufgeführten Dienste und Datensätze sind als Beispiele zu sehen und können durch beliebige Dienste und/oder Datensätze, die einem Nutzer über die Mobilstation bereitgestellt werden können, erweitert oder ersetzt werden.

25

## Patentansprüche

1. Mobilstation (1) eines Mobilkommunikationssystems mit  
- einer Sende- und Empfangseinheit (1a) zum Austauschen von  
5 Signalen mit einer oder mehreren zusätzlichen Mobilstationen und/oder mehreren Basisstationen,  
- einem in die Mobilstation (1) einsetzbaren Identifikationsmodul (SIM) zum Überprüfen einer Nutzungsberechtigung der Mobilstation (1) und zum Aktivieren des Bereitschaftsmodus  
10 der Mobilstation (1),

d a d u r c h g e k e n n z e i c h n e t ,

- dass zumindest einem Dienst und/oder Datensatz, der einem Nutzer über die Mobilstation (1) im Bereitschaftsmodus bereitgestellt und durch den Nutzer abrufbar ist, eine charakteristische Zugriffskennung zugeordnet ist, die charakteristische Zugriffskennung mit einem individuellen Sicherungscode gesichert ist und die Mobilstation (1) zumindest ein Sicherungsmittel (2, 3, 4, 5, 5a, 6, 9, 10, 11, 12, 13)  
15 aufweist, in das durch Eingabe und/oder Übertragung des Sicherungscodes die Zugriffskennung aktivierbar oder deaktivierbar ist und somit der Zugriff auf den Dienst und/oder Datensatz gesperrt bzw. freigegeben ist.  
20

2. Mobilstation (1) eines Mobilkommunikationssystems nach Anspruch 1,  
25

d a d u r c h g e k e n n z e i c h n e t ,

- dass die Zugriffskennung eine oder mehrere Zahlen und/oder ein oder mehrere Buchstaben und/oder ein oder mehrere Sonderzeichen aufweist.  
30

3. Mobilstation (1) eines Mobilkommunikationssystems nach einem der Ansprüche 1 oder 2,

d a d u r c h g e k e n n z e i c h n e t ,

- dass der Sicherungscode eine der nachfolgend aufgeführten Ausführungen oder eine beliebige Kombination der aufgeführten Ausführungen ist:  
35  
- ein PIN-code,

- ein Code aus alphanumerischen Zeichen,
- ein Code aus einem oder mehreren graphischen Symbolen und/oder einem oder mehreren graphischen Zeichen,
- ein biometrisches Merkmal eines berechtigten Nutzers, insbesondere ein Fingerabdruck und/oder ein Augenbild,
- ein akustisches Merkmal eines berechtigten Nutzers, insbesondere die gesprochene Sprache,
- ein drahtlos übertragenes, elektrisches Signal,
- ein Strichcode oder Magnetcode auf einer Identifikations- oder Chipkarte (7).

4. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,

d a d u r c h g e k e n n z e i c h n e t ,

- dass das Sicherungsmittel eine der aufgeführten Ausführungen oder eine beliebige Kombination der aufgeführten Ausführungen zur Eingabe und/oder Übertragung des in Anspruch 3 kombinierten Sicherungscodes ist:
  - eine Tastatur (2),
  - eine berührungssensitive Anzeigefläche (3, 4, 5, 5a), insbesondere ein Touchscreen oder ein Touchpad,
  - ein Sensor, insbesondere ein Fingerabdrucksensor (9),
  - ein zweiter Sensor (12) zum Detektieren eines akustischen Signals, insbesondere der gesprochenen Sprache,
  - ein weiterer Sensor (13) zum Detektieren eines Augenbildes,
  - ein tragbarer Transponder (11) und ein in der Mobilstation angeordneter Empfänger (10),
  - eine Scannervorrichtung (6).

5. Mobilstation (1) eines Mobilkommunikationssystems nach einem der Ansprüche 1 bis 3,

d a d u r c h g e k e n n z e i c h n e t ,

- dass der Sicherungscode zum Aktivieren einer charakteristischen Zugriffskennung und der Sicherungscode zum Deaktivieren der charakteristischen Zugriffskennung unterschiedlich sind.

6. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
5 - dass eine Zugriffskennung mehreren Diensten und/oder Datensätzen zugeordnet ist.
7. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,  
10 dadurch gekennzeichnet,  
- dass jedem Dienst und/oder Datensatz mehrere Zugriffskennungen entsprechend einer Hierarchiestruktur zugeordnet sind.
- 15 8. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
- dass eine Zuordnung der charakteristischen Zugriffskennungen zu den Diensten und/oder Datensätzen und die zugeordnete  
20 te Hierarchiestruktur der übergeordneten Zugriffskennungen vom berechtigten Nutzer veränderbar ist.
9. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,  
25 dadurch gekennzeichnet,  
- dass die den Diensten und/oder Datensätzen zugeordneten Zugriffskennungen und Sicherungscodes in der Mobilstation (1) und/oder im Identifikationsmodul (SIM) gespeichert oder verschlüsselt gespeichert sind.
- 30 10. Mobilstation (1) eines Mobilkommunikationssystems nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
- dass die Mobilstation (1) einen Timer aufweist, der nach  
35 Ablauf einer festlegbaren Zeitdauer, innerhalb der keine Dienste und/oder Datensätze im Bereitschaftsmodus der Mobilstation von einem Nutzer abgefragt werden, Zugriffscodes

automatisch aktiviert und die automatisch zu aktivierenden Zugriffscodes vom berechtigten Nutzer festlegbar sind.

11. Mobilstation (1) eines Mobilkommunikationssystems nach  
5 einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
- dass bei zumindest einer aktivierten Zugriffskennung ankommende Verbindungen im Bereitschaftsmodus der Mobilstation  
15 (1) empfangbar sind.

10

12. Mobilstation (1) eines Mobilkommunikationssystems nach  
einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
- dass die Dienste ein Internetzugang oder ein Mail-Zugang  
15 oder eine Telefonverbindung oder Spiele sind.

13. Mobilstation (1) eines Mobilkommunikationssystems nach  
einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,  
20 - dass die Datensätze eine Adressenliste und/oder eine Telefonnummernliste und/oder Termine und/oder Texte und/oder Sprachaufzeichnungen und/oder Bildaufzeichnungen und/oder Internet oder WAP (Wireless Access Protocol) -Inhalte  
sind.

25

14. Verfahren zum Zugreifen auf einen Dienst und/oder einen Datensatz, die im Bereitschaftsmodus einer Mobilstation (1) bereitgestellt werden und von einem Nutzer abgerufen werden,  
dadurch gekennzeichnet,  
30 - dass zumindest einem Dienst und/oder Datensatz eine charakteristische Zugriffskennung zugeordnet wird, die über einen Sicherungscode, der in Sicherungsmittel (2, 3, 4, 5, 5a, 6, 9, 10, 11, 12, 13) der Mobilstation (1) eingegeben und/oder übertragen wird, aktiviert oder deaktiviert wird und ein  
35 Zugriff auf den Dienst und/oder Datensatz gesperrt bzw. freigegeben wird.

15. Verfahren nach Anspruch 14,

dadurch gekennzeichnet,

- dass die Zugriffskennung aus einer oder mehreren Zahlen und/oder einem oder mehreren Buchstaben und/oder einem oder mehreren Sonderzeichen kombiniert wird.

16. Verfahren nach einem der Ansprüche 14 oder 15,

dadurch gekennzeichnet,

- dass als Sicherungscode eine der nachfolgenden Ausführungen oder eine beliebige Kombination der Ausführungen gewählt

wird:

- ein PIN-code, der insbesondere zum Aktivieren des Bereitschaftsmodus der Mobilstation (1) eingegeben wird,
- ein Code aus alphanumerischen Zeichen,
- ein Code aus einem oder mehreren graphischen Symbolen und/oder einem oder mehreren graphischen Zeichen,
- ein biometrisches Merkmal eines berechtigten Nutzers, insbesondere ein Fingerabdruck und/oder ein Augenbild,
- ein akustisches Merkmal eines berechtigten Nutzers, insbesondere die gesprochene Sprache,
- ein drahtlos übertragenes, elektrisches Signal,
- ein Strichcode oder Magnetcode auf einer Identifikations- oder Chipkarte (7).

17. Verfahren nach einem der Ansprüche 14 bis 16,

dadurch gekennzeichnet,

- dass der Sicherungscode mittels einem der nachfolgend aufgeführten Sicherungsmittel oder einer beliebigen Kombination der Sicherungsmittel eingegeben und/oder übertragen wird:

- eine Tastatur (2),
- eine berührungssensitive Anzeigefläche (3, 4, 5, 5a), insbesondere ein Touchscreen oder ein Touchpad,
- ein Sensor zum Detektieren biometrischer Merkmale, insbesondere ein Fingerabdrucksensor (9) oder ein Augenbildsensor (13),
- ein zweiter Sensor (12) zum Detektieren eines akustischen Merkmals, insbesondere der gesprochenen Sprache,

27

- ein tragbarer Transponder (11) und ein in der Mobilstation (1) angeordneter Empfänger (10),
- eine Scannervorrichtung (6).

5 18. Verfahren nach einem der Ansprüche 14 bis 16,

dadurch gekennzeichnet,

- dass zum Aktivieren einer charakteristischen Zugriffskennung und zum Deaktivieren dieser Zugriffskennung verschiedene Sicherungscodes verwendet werden.

10

19. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass einer Zugriffskennung mehrere Dienste und/oder Datensätze zugeordnet werden.

15

20. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass jedem Dienst und/oder Datensatz mehrere Zugriffskennungen zugeordnet werden.

20

21. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass eine Zuordnung der charakteristischen Zugriffskennungen zu den Diensten und/oder Datensätzen und eine zugeordnete Hierarchiestruktur von übergeordneten Zugriffskennungen zu charakteristischen Zugriffskennungen vom berechtigten Nutzer festgelegt werden.

25

22. Verfahren nach einem der vorhergehenden Ansprüche,

30 dadurch gekennzeichnet,

- dass die den Diensten und/oder Datensätzen zugeordneten Zugriffskennungen und Sicherungscodes in der Mobilstation (1) und/oder im Identifikationsmodul (SIM) gespeichert oder verschlüsselt gespeichert werden.

35

23. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass mittels eines Timers eine Zeitdauer festgelegt wird, nach deren Ablauf Zugriffskennungen automatisch aktiviert werden, sobald innerhalb dieser Zeitdauer keine Dienste und/oder Datensätze von einem Nutzer abgefragt werden und  
5 die automatisch zu aktivierenden Zugriffskennungen vom berechtigten Nutzer vorab festgelegt werden.

24. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,

- 10 - dass bei zumindest einer aktivierten Zugriffskennung ankommende Verbindungen im Bereitschaftsmodus der Mobilstation (1) empfangen werden.

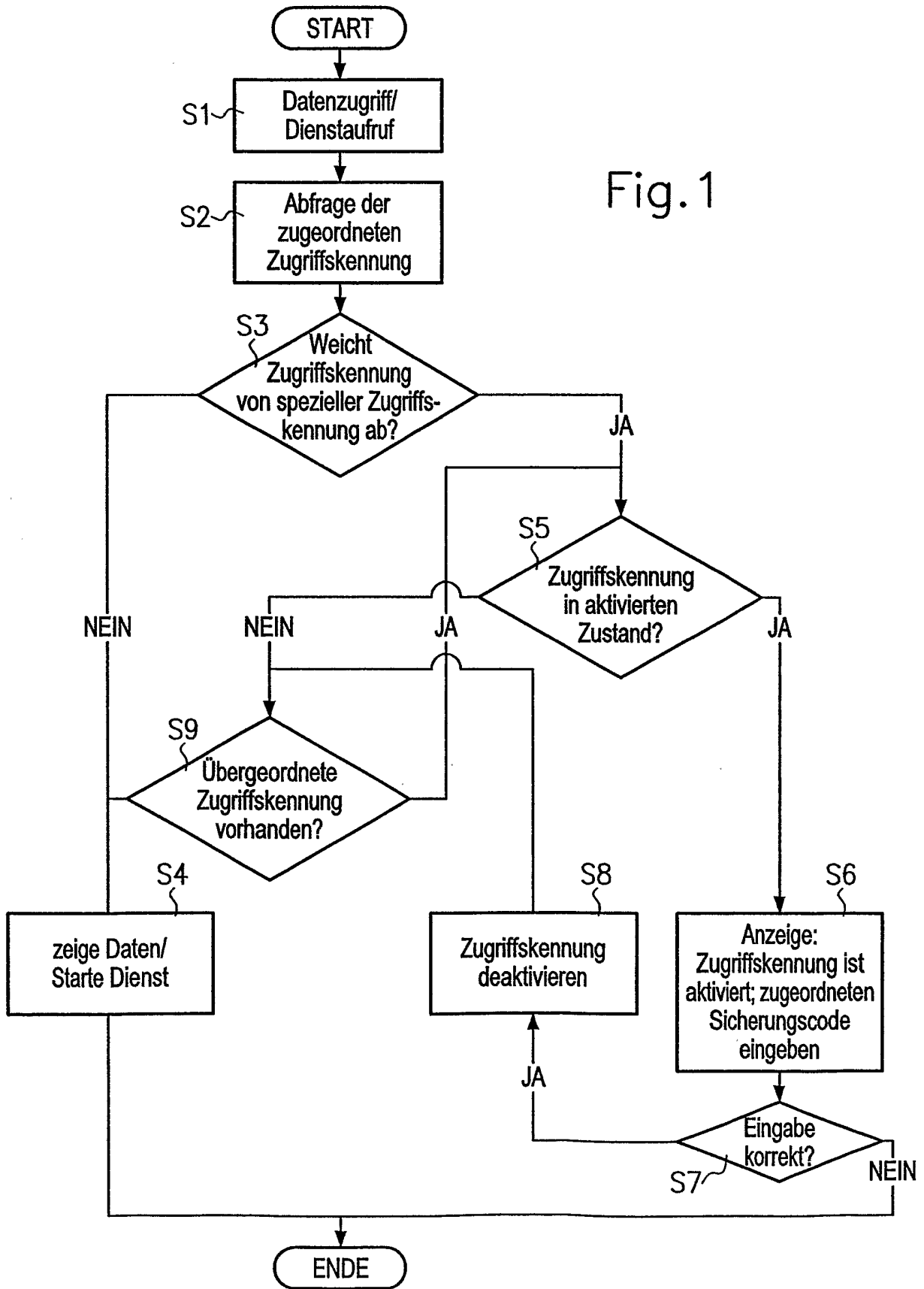
25. Verfahren nach einem der vorhergehenden Ansprüche,  
15 dadurch gekennzeichnet,

- dass als Dienste Spiele und/oder ein Mail-Zugang und/oder ein Internetzugang und/oder eine Telefonverbindung bereitgestellt werden.

20 26. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet,

- dass als Datensätze eine Adressenliste und/oder eine Telefonnummernliste und/oder Termine und/oder Texte und/oder Sprachaufzeichnungen und/oder Bildaufzeichnungen und/oder  
25 Internet- oder WAP-Inhalte bereitgestellt werden.

Fig. 1



2/5

Dienst und /oder Datensatz	Zugriffskennung	Zustand der Zugriffskennung	übergeordnete Zugriffskennung	zugeordneter Sicherungscode zur Zugriffskennung
Jahreskalender	0	-	-	-
private Telefonnummern	1	aktiviert	3;4	01
dienstl. Telefonnummern	2	deaktiviert	3;4	11
Adressenliste	3	aktiviert	-	2134
e-mail	4	aktiviert	3	225
Internet	5	aktiviert	-	34

Fig.2

Dienst und /oder Datensatz	Zugriffskennung	Zustand der Zugriffskennung	übergeordnete Zugriffskennung	zugeordneter Sicherungscode zur Zugriffskennung
private Telefonnummern	1	aktiviert	3; 4	1815
dienstl. Telefonnummern	2	deaktiviert	3; 4	53
wichtige dienstl. Telefonnummern	2	deaktiviert	4	53
Adressenliste	3	aktiviert	4	A7
Datensatz 1	4	aktiviert	-	graf. Symbol (Unterschrift)
Termine	5	aktiviert	4	24
e-mail	6	aktiviert	7	?5?
SMS	7	aktiviert	-	elektrisches Signal
Sprachaufzeichnung	8	aktiviert	7	Strichcode
Bildaufzeichnung	9	aktiviert	8; 7	BILD
Internet	10	aktiviert	-	Fingerabdruck
Spiele	11	aktiviert	-	Spracheingabe des Wortes "SPIELE"

Fig.3

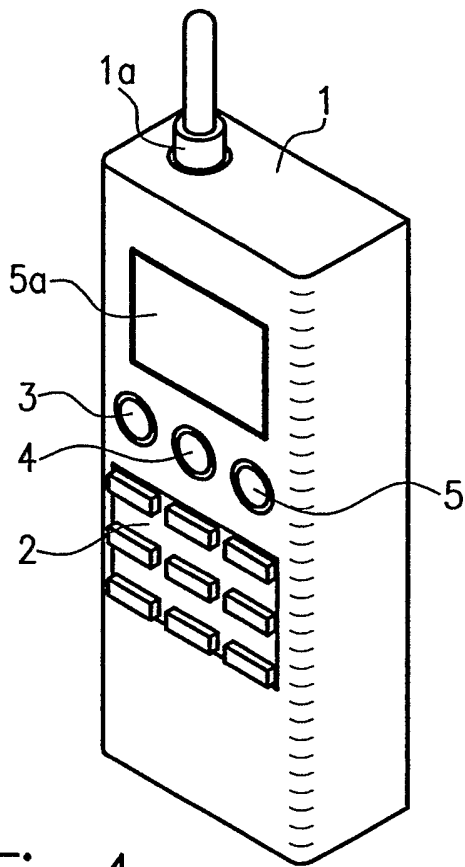


Fig. 4

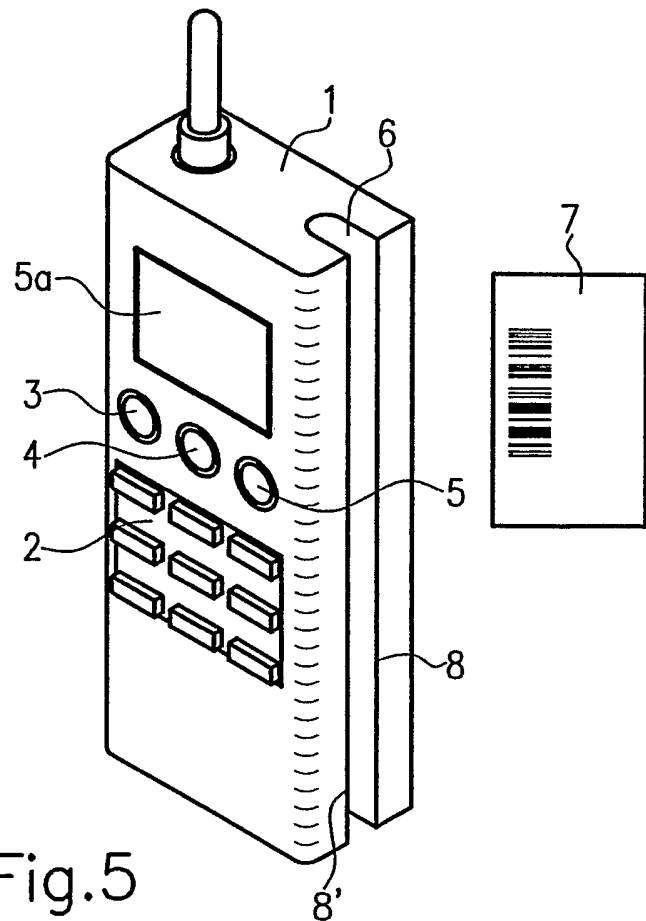


Fig. 5

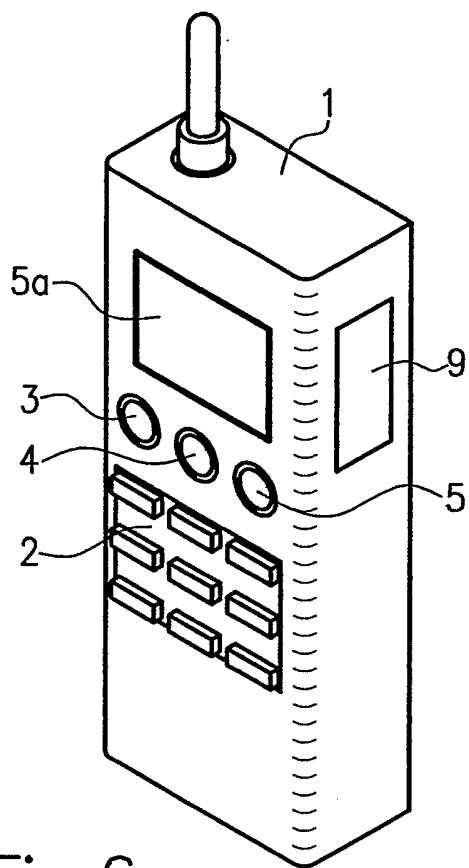


Fig. 6

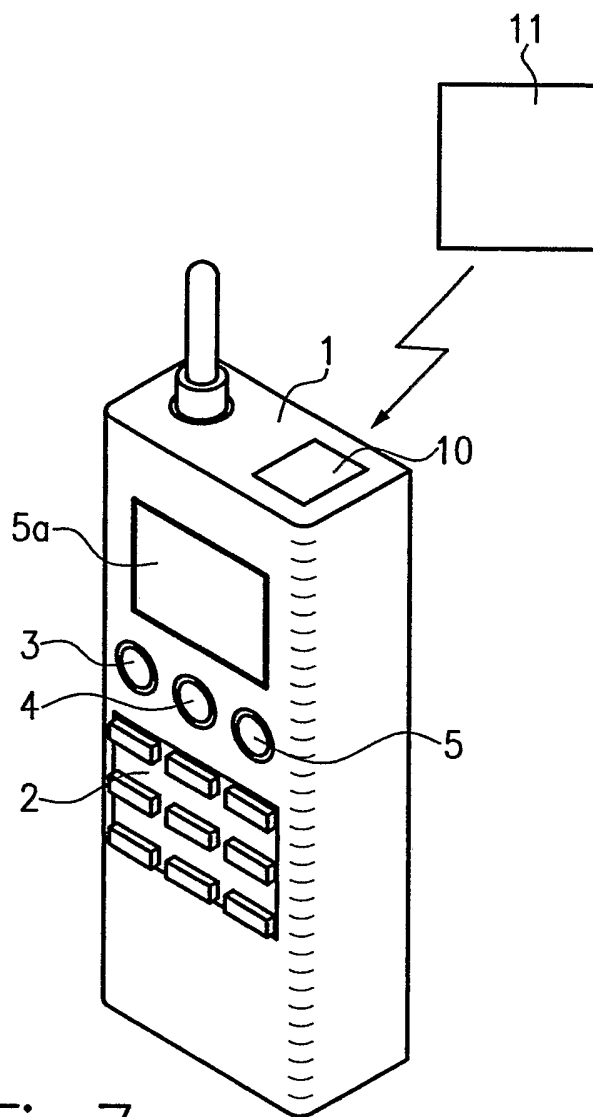


Fig. 7

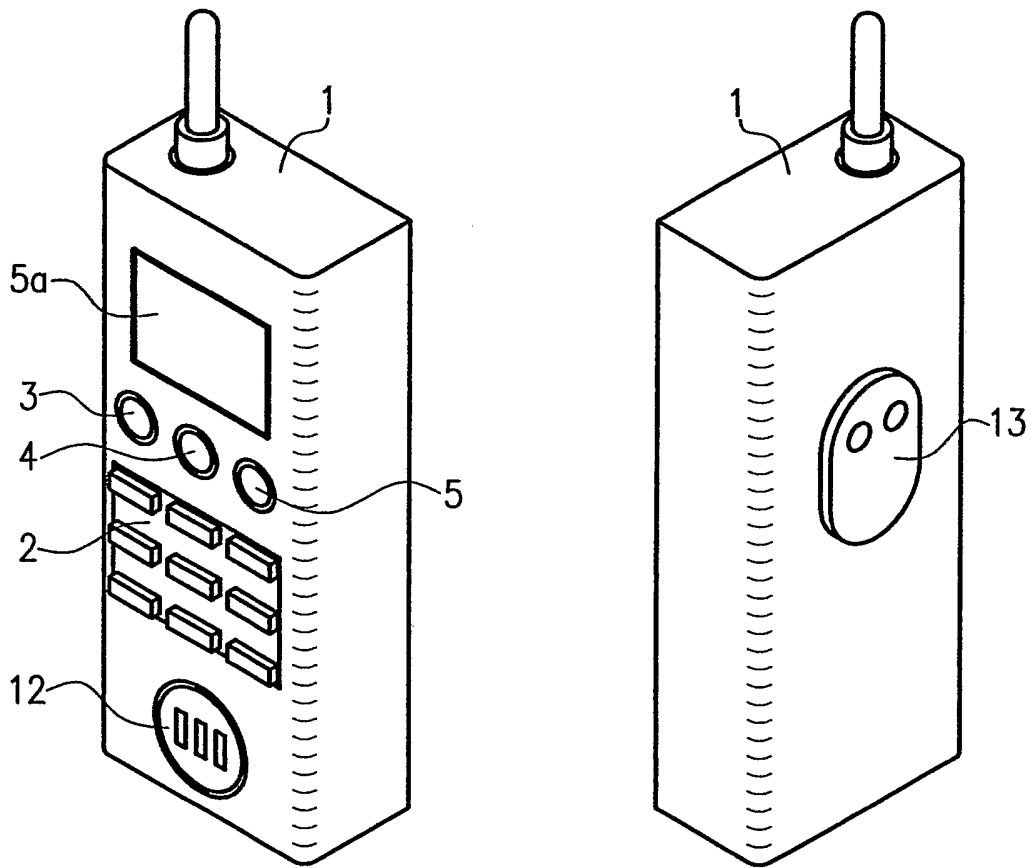


Fig.8