(19) **Bundesrepublik Deutschland**
**Deutsches Patent- und Markenamt**

(10) **DE 699 25 391 T2** 2006.02.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 932 317 B1**
(21) Deutsches Aktenzeichen: **699 25 391.8**
(96) Europäisches Aktenzeichen: **99 400 079.2**
(96) Europäischer Anmeldetag: **14.01.1999**
(97) Erstveröffentlichung durch das EPA: **28.07.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **25.05.2005**
(47) Veröffentlichungstag im Patentblatt: **02.02.2006**

(51) Int Cl.[8]: ***H04Q 7/32*** (2006.01)
***H04L 9/32*** (2006.01)

(30) Unionspriorität:
**9800771** **26.01.1998** **FR**

(84) Benannte Vertragsstaaten:
**CH, DE, ES, FI, FR, GB, IT, LI, SE**

(73) Patentinhaber:
**Alcatel, Paris, FR**

(74) Vertreter:
**Dreiss, Fuhlendorf, Steimle & Becker, 70188 Stuttgart**

(72) Erfinder:
**Vasnier, Frederic, 92700 Colombes, FR;**
**Lelong-Gilbert, Anna-Gaelle, 78220 Viroflay, FR;**
**Hubbe, Pascal, 75014 Paris, FR; Choquet, Christophe, 75015 Paris, FR**

(54) Bezeichnung: **Verfahren zur verschlüsselten Datenübertragung zwischen einem Teilnehmer-Identifikationsmodul und einem Mobilfunkendgerät**

## Beschreibung

**[0001]** Die Erfindung fällt in den Bereich der Funksysteme und vor allem, aber nicht ausschließlich, von derartigen Systemen wie GSM (engl. Global System for Mobile communications) und DCS 1800 (engl. Digital Cellular System).

**[0002]** In einem derartigen System kommuniziert der Teilnehmer allgemein gesehen mit einer Mobilstation, die von einem mobilen Endgerät gebildet wird, das mit einem Teilnehmeridentifizierungsmodul, üblicherweise SIM-Karte (im GSM-Standard engl. Subscriber Identity Module) genannt, zusammenwirkt.

**[0003]** Die GSM-Empfehlung 11.11 empfiehlt, die Daten, die mit den von den Funknetzen bereitgestellen Diensten verbunden sind, ebenso wie die Daten, die mit der Teilnehmeridentifizieung verbunden sind, in den Speicherbereichen der SIM-Karte zu speichern.

**[0004]** Der europäische Telekommunikationsstandard ETS (engl. Eu ropean Telecommunication Standard) definiert die Schnittstelle zwischen dem Teilnehmeridentifizierungsmodul und dem mobilen Endgerät.

**[0005]** Den GSM-Empfehlungen 11.11 und 11.14 zufolge wird Werkzeugsatz, der sich auf den Einsatz der SIM-Karte bezieht und im Englischen mit SIM Application Toolkit sowie im Folgenden mit SIM-Werkzeugsatz bezeichnet wird, verwendet. Dieser SIM-Wrkzeugsatz vereint eine Reihe von Anwendungen und verbundenen Verfahren, die bei Kommunikationssitzungen zwischen einem mobilen Endgerät und einer ihm zugeordneten SIM-Karte verwendet werden können. Die Kommunikation zwischen einem mobilen Endgerät und einer zugeordneten SIM-Karte ist vor allem in der Patentanmeldung DE 195 27 715 beschrieben.

**[0006]** Im Allgemeinen ist die SIM-Karte eine Chipkarte zur Personalisierung der Mobilstation. Die Personalisierung der Mobilstation ist nämlich bei tragbaren mobilen Endgeräten notwendig, die ein höheres Verlust- oder Diebstahlrisiko aufweisen, was zu einer betrügerischen Anwendung führen kann.

**[0007]** Die dem Teilnehmer zur Begrenzung des Risikos einer derartigen betrügerischen Anwendung vorgeschlagene Lösung besteht in der Verwendung einer herausnehmbaren SIM-Karte, die der Teilnehmer aus dem mobilen Endgerät immer dann herausnehmen kann, wenn er sich von demselben trennt. Ohne SIM-Karte kann das mobile Endgerät nur noch zu einer beschränkten Anzahl von Kommunikationsarten verwendet werden, insbesondere für Notrufe.

**[0008]** Allerdings wird das Problem durch diese Maßnahmen nicht vollständig gelöst. So kann ein Betrüger, der im Besitz eines mobilen Endgeräts ist, immer noch die diesem normalerweise zugeordnete SIM-Karte simulieren, um dieses mobile Endgerät in betrügerischer Absicht zu benutzen, eventuell nach dem Abfangen von Nachrichten, die regelmäßig zwischen diesem mobilen Endgerät und seiner SIM-Karte ausgetauscht wurden.

**[0009]** Es ist zu befürchten, dass insbesondere seit der Kommer zialisierung sogenannter Prepaid-Karten nach derartigen betrü gerischen Anwendungen gesucht wird. Nach der (betrügerischen) Erkennung, dass eine Station eine derartige Karte enthält, wird die Anwendung der Station nämlich freigegeben, da davon ausgegangen wird, dass die Kommunikationszeit auf dem im voraus bezahlten und in der Karte eingeschlossenen Konto verbucht wird. Bei im voraus bezahlten Konten, die mit einer im voraus bezahlten Karte geladen werden, ist die Situation ähnlich (dann betrifft der Betrug die Ladung des Kontos).

**[0010]** Aufgabe der vorliegenden Erfindung ist es, für dieses Problem eine Lösung anzubieten, die so beschaffen ist, jedweden Betrug so schwierig zu gestalten, dass er unwahrscheinlich ich wird.

**[0011]** Demzufolge hat die Erfindung zu diesem Zweck ein Verfahren zur Informationsübertragung zwischen einem Teilnehmeridentifizierungsmodul und einem mobilen Endgerät zur Aufgabe, die eine Station eines Funksystems bilden. Erfindungsgemäß wird mindestens ein Teil der zwischen dem Modul und dem Endgerät übertragenen Informationen mittels eines Schlüssels, der sowohl in dem Modul als auch in dem Endgerät verwendet wird, durch Verschlüsselung geschützt. Dieser Schlüssel wird mindestens zum Teil durch ein periodisch variables Datenelement des Systems festgelegt.

**[0012]** Erfindungsgemäß ist das periodisch variable Datenelement eine dem Funksystem eigene Zeitgeberfunktion.

**[0013]** Vorzugweise wird der Schlüssel mindestens teilweise durch ein anderes, der Mobilstation eigenes Datenelement festgelegt.

**[0014]** Weiterhin werden die den Schlüssel festlegenden Daten vorzugweise sowohl in dem Modul als auch in dem Endgerät bei jeder durch Verschlüsselung geschützten Informationsübertragung zusammengestellt.

**[0015]** Eine weitere Aufgabe der Erfindung besteht in einem mobilen Endgerät und einer SIM-Karte, die jeweils aufeinander abgestimmt sind, um das Verfahren zur Übertragung verschlüsselter Informationen anwenden zu können.

**[0016]** Andere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung einer Ausführungsform der Erfindung, die als einfaches, nicht beschränkendes Beispiel gegeben wird und sich auf die anliegenden Zeichnungen bezieht bei denen:

**[0017]** Fig. 1 ein vereinfachtes Schema einer Ausführungsform eines erfindungsgemäßen Teilnehmeridentifizierungsmoduls darstellt;

**[0018]** Fig. 2 ein vereinfachtes Schema einer Ausführungsform eines erfindungsgemäßen mobilen Endgeräts darstellt, das dazu bestimmt ist, mit dem Teilnehmeridentifizierungsmodul von Fig. 1 zusammenzuwirken;

**[0019]** Fig. 3 ein vereinfachtes Ablaufschema einer Ausführungsform des erfindungsgemäßen Verfahrens zur Informat übertragung ist;

**[0020]** Fig. 4 eine Nachricht darstellt, die im Rahmen des Verfahrens von Fig. 3 von einem mobilen Endgerät zu einem Teilnehmeridentifizierungsmodul übertragen wird;

**[0021]** Fig. 5 Mittel darstellt, welche die Ausstattung des Teilnehmeridentifizierungsmoduls von Fig. 1 mit einem Verschlüsselungsschlüssel ermöglichen.

**[0022]** Die folgende Beschreibung behandelt die Umsetzung der Erfindung im speziellen Fall eines Funksystems nach GSM-Standard. ES versteht sich von selbst, dass ein Fachmann die obigen Prinzipien nicht nur auf das bereits erwähnte System DCS 1800 anwenden können wird, sondern auch auf andere Arten von Funksystemen.

**[0023]** Fig. 1 ist eine allgemeine grafische Darstellung einer Ausführungsform einer SIM-Karte **10**, die vor allem von einem Trägerelement **11** gebildet wird, das die Verbindungskontaktbe reiche **12** und einen Multichip **13** trägt. Dieser weist vor allem Mittel **14** zur Datenverarbeitung (typischerweise einen Mikroprozessor) auf, die mit einem bidirektionalen Bus gekoppelt sind, an den die Kontaktbereiche **12** über eine Übertragungseinheit **16** sowie einen Speicher **17** angeschlossen sind. Eine Verschlüsselungseinheit **18** ist mit der Übertragungseinheit **16** gekoppelt, und der Speicher **17** weist einen Bereich **19** auf, der für die Verschlüsselungsinformation zuständig ist.

**[0024]** Der Speicher **17** weist auf klassische Weise einen Festspeicher **171** auf, in dem einem Telefonabonnement zugeordnete Daten die den Betrieb einer Mobilstation mit SIM-Karte **10** ermöglichen, sowie die zum Betrieb des Mikroprozessors **14** notwendigen Programme eingetragen sind. Diese Daten können dort vom Provider eines Funknetzes oder von einem Verkäufer einge tragen werden und haben im allgemeinen einen permanenten Charakter. Einige Daten jedoch sind durch spezielle Einwirkung des Mikroprozessors **14** veränderbar und sind damit teilpermanent. Der Speicher **17** weist ebenfalls einen Arbeitsspeicher **172** auf, der von dem Mikroprozessor zum Speichern von Daten aus einem mobilen Endgerät, in dem sich die SIM-Karte **10** befindet, sowie von den Daten, die sich aus den Berechnungen des Mikroprozessors **14** ergeben, verwendet wird, von denen einige an das mobile Endgerät übertragen werden müssen. Der Speicherbereich **19** wird in vorteilhafter Weise zwischen dem Festspeicher **171** und dem Arbeitsspeicher **172** aufgeteilt, wie im folgenden unter Bezugnahme auf Fig. 5 erläutert werden wird.

**[0025]** Die allgemeine Funktionsweise der zunächst inaktiven SIM- Karte besteht in der Durchführung einer vom mobilen Endgerät gemäß dem obig erwähnten SIM-Werkzeugsatz initialisierten Sitzung, wobei von den Kontaktbereichen **12** und der Übertragungseinheit **16** Datein an den Mikroprozessor **14** übertragen werden. Als Antwort arbeitet der mit dem Speicher **17** verbundene Mikroprozesor **14** ein Programm aus dem Festspeicher **171** ab, das bewirkt, dass von ihm die vom mobilen Endgerät gelieferten Daten im Arbeitsspeicher **172** gespeichert, diese Daten bearbeitet und andere Daten aus dem Festspeicher **171** abgerufen werden, um Bearbeitungsergebnisse vorzubereiten, die im Arbeitsspeicher **172** gespeichert werden. In diesem Zusammenhang bewirkt der Mikroprozessor **14** ebenfalls, dass Ergebnisdaten, die im Arbeitsspeicher **172** vorbereitet wurden, von der Übertragungseinheit **16** an das mobile Endgerät übertragen werden. Sobald diese eventuell mehrfachen Datenübertragungen abgeschlossen sind, wird die Sitzung beendet und die SIM-Karte wird wieder inak tiv.

**[0026]** Erfindungsgemäß wird die Karte durch Hinzufügen der Ver chlüsselungseinheit **18** und des Speicherbereichs für die Verschlüsselungsinformation **19** so ausgestattet, dass die eben erwähnten Datenübertragungen durch Verschlüsselung geschützt sind. Die Verschlüsselungstechnik ist gut bekannt und wird hier nicht beschreiben. Sie benötigt als Schlüssel eine Abfolge vertraulicher Verschlüsselungsdaten, die in der Verschlüsselungseinheit **18** mit den zu übertragenden Daten kombiniert werden, um eine Abfolge Signale zu liefern, die unverständlich sind, außer demjenigen, der den Schlüssel besitzt, um die umgekehrte Operation – die Entschlüsselung – durchzuführen, wodurch die ursprüngliche Information wiederhergestellt wird. Der Schlüssel wird in der Verschlüsselungseinheit **18** mit Hilfe einer Schlüsselinformation erzeugt, die vom Mikroprozessor **14** vorbereitet und ihm vom Bus **15** mitgeteilt werden kann. Dieses Detail wird im Rahmen der Beschreibung des erfindungsgemäßen Verfahrens zur Informationsübertragung unter Bezugnahme auf Fig. 3 weiter ausgeführt werden.

**[0027]** Fig. 2 zeigt das allgemeine Schema einer Ausführungsform eines mobilen Endgeräts **20**, das einem Speicher **23** zugeordnete Mittel zur Datenverarbeitung **21** (typischerweise einen Mikroprozessor) aufweist, die über einen bidirektionalen Bus die anderen Mittel des Endgeräts steuern.

**[0028]** Der Mikroprozessor **21** steuert vor allem verschiedene Schnittstellenvorrichtungen **24** bis **26** jeweils mit einem Bildschirm **28**, einer Tastatur **29** und einem Mikrofon-Lautsprechersatz **210**. Er steuert insbesondere eine Übertragungsvorrichtung **27**, die dem Kontaktelementblock **211** zugeordnet ist, dessen Kontaktelemente mit den Kontaktbereichen einer im Endgerät befindlichen SIM-Karte elektrisch in Kontakt tre ten. Erfindungsgemäß wird an die Übertragungsvorrichtung **27** zusätzlich eine Verschlüsselungsvorrichtung **212** gekoppelt, und der Speicher **23** weist einen Slot **231** für die Verschlüsselungsinformation auf.

**[0029]** Die Funktionsweise dieses mobilen Endgeräts **20** wird nicht beschrieben werden, da dies aus dem Rahmen der vorliegenden Erfindung fallen würde. Es ist ausreichend, wenn in diesem Rahmen ausgeführt wird, dass der Betrieb verlangt, dass die in der SIM-Karte gespeicherten Informationen verwendet werden. Der Mikroprozessor **21** des mobilen Endgeräts initialisiert demnach gemäß dem oben angeführten SIM-Werkzeugsatz eine Sitzung, wobei von der Übertragungsvorrichtung **27** und den Kontakteleentblöcken **211** in beide Richtungen Datenübertragungen innerhalb des Rahmen vorgenommen werden, der sich aus der Beschreibung zu Fig. 1 ergibt.

**[0030]** Erfindungsgemäß ist das mobile Endgerät durch Hinzufügen der Verschlüsselungsvorrichtung **212** und des Slots für den Verschlüsselungsinformationsspeicher **231** so ausgestattet, dass bestimmte Datenübertragungen, wie bereits erwähnt wurde, durch Verschlüsselung geschützt werden.

**[0031]** Fig. 3 veranschaulicht, wie die Erfindung in einem Verfahren zur Informationsübertragung zwischen einem Teilnehmeridentifizierungsmodul wie der SIM-Karte von Fig. 1 und einem mobilen Funk-Endgerät gemäß Fig. 2 umgesetzt werden kann.

**[0032]** Man versetze sich beispielsweise in den Fall eines Anwenders, der die Tasten seiner Tastatur **29** drückt, um einen abgehenden Anruf zu tätigen. Er beendet, indem er eine Betätigungstaste drückt, und in diesem Augenblick muss das Endgerät die SIM-Karte verständigen um zu überprüfen, ob der Anruf genehmigt ist oder nicht, und bei einer Prepaid-Karte, ob das verbleibende Guthaben den Abgang des Anrufs erlaubt.

**[0033]** In einem ersten Schritt **31** ruft das mobile Endgerät den SIM-Werkzeugsatz für eine RUF-STEUERUNG genannte Sitzung an. Diese Sitzung weist mehrere Teile auf. Der erste, mit BENUTZER-EINGANG bezeichnete Teil, beginnt mit einem Schritt **31**, ANRUF genannt, der die Aktivierung der SIM-Karte und den Versand einer Nachricht **41** durch das mobile Endgerät an die SIM-Karte (genauer gesagt, an den Mikroprozessor der Karte) umfasst, die von Fig. 4 veranschaulicht wird. Diese Nachricht weist unter anderem ein Datenelement ST, das sie als einem SIM-Befehl zugehörig identifiziert, ein Datenelement TS, das die Art der Sitzung identifiziert (hier: BENUTZEREINGANG), eine Anzeige S, die sie als erste Nachricht einer Sitzung identifiziert und schließlich ein Datenelement TIME auf. Dieses Datenelement TIME ist eine zeitabhängig variable, dem Funksystem eigene Information, so dass es nicht notwendig ist, Mittel zu deren Erzeugung vorzusehen und es ausreicht, sie im mobilen Endgerät auf einer Vorrichtung abzulesen, die sie bereits für einen anderen Verwendungszweck enthält; hierbei handelt es sich in vorteilhafter Weise um die Zeitinformation, auch GSM-Zeitgeber genannt, welche die Elemente T1, T2, T3 aufweist, die im GSM-System gut bekannt sind und von den Empfehlungen 05.02 und 05.10 der GSM-Norm bestimmt werden. Der Schritt **31** umfasst selbstverständlich auch den Empfang dieser Nachricht in der SIM-Karte. Dieser Schritt wird ohne Verschlüsselung durchgeführt, das heißt dass die Verschlüsselungsvorrichtung **212** des mobilen Endgeräts und die Verschlüsselungseinheit **18** der SIM-Karte nicht aktiv sind und nicht in die Übertragung eingreifen.

**[0034]** Die Übertragung dieser Nachricht führt zu einem Schritt **32**, SCHLÜSSELBERECHNUNG genannt, welcher die Berechnung eines Verschlüsselungsschlüssels gemäß den Anordnungen umfasst, die von Fig. 5 veranschaulicht werden. Fig. 5 bezieht sich insbesondere auf die Durchführung dieser Berechnung in der SIM-Karte, wobei noch zu sehen sein wird, dass dieselbe Berechnung auch im mobilen Endgerät durchgeführt wird. Ein Bereich **171.1** des Festspeichers **17** enthält einen Quellschlüssel CM. Dieser ist dem Hersteller oder dem Provider zueigen und wurde dort gleichzeitig wie die anderen, dem Telefonvertrag zugeordneten Daten eingetragen. Ein anderer Bereich **171.2** des Speichers **17** enthält eine IMEI-Kennung (in der Terminologie des GSM-Systems engl. International Mobile Equipment Identity), das heißt eine Nummer, die dem mobilen Endgerät zueigen ist und in die Karte bei Abschluss des Abonnementsvertrags eingetragen wird, wie bereits erläutert wurde. Abschließend, während Schritt **31**, wird das Datenelement TIME in einem Bereich **172.1** des Arbeitsspeichers **172** temporär registriert. Diese drei Elemente werden in einer Kombinationsvorrichtung **51** kombiniert, um in **52** eine Information zu produzieren, die den Schlüssel CS generiert. Die Kombinationsvorrichtung **51** kann in der Verschlüsselungsein-

heit **18** verkabelt sein, wobei ihr der Mikroprozessor die obigen drei Elemente schickt, oder sie kann programmiert sein, um vom Mikroprozessor **14** ausgeführt zu werden, der dann die Information CS direkt an die Verschlüsselungseinheit **18** liefert.

**[0035]** Parallel dazu, was nicht detailliert beschrieben werden muss, läuft dasselbe Verfahren im mobilen Endgerät ab, wobei die Slots, die durch **231** des Speichers **23** geschlossen dargestellt werden, auf dieselbe Art und Weise die obigen drei Elemente beinhalten und Mittel zu deren Kombination gemäß Fig. 5 zu einer schlüsselgenerierenden Information, die schließlich in der Verschlüsselungseinheit **212** zur Verfügung steht.

**[0036]** Schritt **33**, AR genannt, besteht danach im wesentlichen darin, ein Signal der Empfangsbestätigung und des Befehls zur Durchführung der verschlüsselten Übertragung von der SIM-Karte an das mobile Endgerät zu übertragen. Damit werden die Verschlüsselungseinheit **18** und die Verschlüsselungsvorrichtung **212** im Hinblick auf die in beide Richtungen durch die Schnittstelle Endgerät/SIM-Karte übertragenen Daten gleichzeitig ak tiviert, die sich in den Datenübertragungsweg zwischen der Übertragungseinheit **16** oder der Übertragungsvorrichtung **27** und dem Quell- oder Emfangselement, Mikroprozessor **1** oder Speicher **172** in der SIM-Karte, Mikroprozessor **21** oder Speicher **23** im mobilen Endgerät, zwischenschalten.

**[0037]** Ab diesem Augenblick beinhalten die Schritte **34** ... **35**, die mit ÜBERTRAGUNG 1, ..., ÜBERTRAGUNG N bezeichnet werden, die Datenübertragung in verschlüsselter Form. Die Übertragung zwischen der SIM-Karte kann nicht mehr verwendet werden, auch wenn sie auf Ebene der Kontaktbereiche **12** oder der Kontaktelemente **211** zwischengeschaltet ist. Es ist nunmehr nicht mehr möglich, diese zu fälschen. Das Ziel der Erfindung ist damit erreicht.

**[0038]** Die schlüsselerzeugenden Informationen, die in der SIM-Karte und im mobilen Endgerät dieselben sind, werden in einer schlüsselerzeugenden Vorrichtung wie einem ReaktionsSchiberegister sowohl in der Verschlüsselungseinheit **18** als auch in der Verschlüsselungsvorrichtung **212** umgesetzt und stellen zwei identische Schlüssel her, von denen einer zur Verschlüsselung am Endpunkt der Sendung und der andere zur Entschlüsselung am Endpunkt des Empfangs verwendet wird

**[0039]** Fig. 3 veranschaulicht nach den Schritten **31** bis **35**, die bereits beschrieben wurden und sich auf einen mit BENUTZEREINGANG bezeichnete Datenübertragung beziehen, eine andere Übertragung mit der Bezeichnung RUFAUFBAU, die zu den im SIM-Werkzeugsatz vorgesehenen Übertragungen gehört, wo ein Schritt **36** mit der Bezeichnung GENEHMIGTER RUF den verschlüsselten Versand einer Nachricht, die mitteilt, dass der von Schritt **31** bestimmte Ruf genehmigt ist, umfasst. Daraus ergibt sich die tatsächliche Sendung des entsprechenden Rufs durch das mobile Endgerät gemäß dem GSM-System. Parallel dazu steuert ein anderer, mit ANZEIGE bezeichneter Schritt **37** einer TEXTANZEIGE-Übertragung die Anzeige eines dem aktuellen Ruf entsprechenden Textes auf dem Bildschirm des mobilen Endgeräts. In einem Schritt **38** am Ende der Sitzung, der mit ENDE bezeichnet wird, werden die Verschlüsselungseinheit **18** und die Verschlüsselungsvorrichtung **212** deaktiviert. Der zuvor angewendete Schlüssel ist nicht mehr verwendbar. Die Sitzung ist geschlossen. Es müsste eine weitere Sitzung nach dem soeben beschriebenen Modell stattfinden.

**[0040]** Es versteht sich von selbst, dass die vorstehenden Erläuterungen weitere Varianten umfassen könnten, ohne jedoch den Rahmen der Erfindung zu sprengen, so wie diese in den Ansprüchen bestimmt ist. Insbesondere die Zusammensetzung des Schlüssels kann unterschiedlich sein von dem Augenblick an, in dem er eine variable, systemabhängige Information aufweist. Damit könnte die IMEI-Nummer von einer anderen, dem Abonnement entsprechenden Nummer ersetzt werden und in der SIM-Karte wie im mobilen Endgerät zur Verfügung stehen. Eine andere variable Information des Systems (Entfernung von der Basisstation, Sendepegel usw.) könnte den GSM-Zeitgeber ersetzen. Die Art und Weise der Verwendung der schlüsselerzeugenden Information könnte unterschiedlich sein, wobei zum Beispiel der Mikroprozessor der Karte und des Endgeräts die Verschlüsselung anstelle eines bestimmten Organs wie der Einheit **18** oder der Vorrichtung **212** komplett übernehmen könnten. Auch beruht die Um setzung eines berechneten Schlüssels auf der Grundlage einer Sitzung des SIM-Werkzeugsatzes. Selbstverständlich ist es durch Anpassungen, die für einen Fachmann naheliegend sind, möglich, eine andere Basis zu verwenden, das heißt entweder eine einfache Übertragung oder im Gegensatz dazu eine gesamte Aktivitätsperiode des Endgeräts. Die obigen Beispiele stehen in der Tat nur für bevorzugte Lösungen im Rahmen der beabsichtigen Anwendung.

## Patentansprüche

1. Verfahren zur Informationsübertragung zwischen einem Teilnehmeridentifizierungsmodul (**10**) und einem mobilen Endgerät (**20**), die Station eines Funksystems bilden, wobei mindestens ein Teil der zwischen dem Modul und dem Endgerät übertragenen Informationen mittels eines Schlüssels (CS), der sowohl in dem Modul (**10**) als auch in dem Endgerät (**20**) verwendet wird, durch Verschlüsselung geschützt ist, **dadurch gekennzeichnet**, dass der Schlüssel (CS) mindestens für einen Teil (TIME)

durch ein periodisch variables Datenelement (T1, T2, T3) des Systems festgelegt ist.

2. Verfahren zur Informationsübertragung nach Anspruch 1, dadurch gekennzeichnet, dass das periodisch variable Datenelement (T1, T2, T3) eine dem Funksystem eigene Zeitgeberfunktion ist.

3. Verfahren zur Informationsübertragung nach Anspruch 1, oder 2, dadurch gekennzeichnet, dass der Schlüssel (CS) für einen anderen Teil mindestens durch ein der mobilen Station eigenes Datenelement (IMEI) festgelegt ist.

4. Verfahren zur Informationsübertragung nach nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die den Schlüssel (CS) festlegenden Daten sowohl in dem Modul (**10**) als auch in dem Endgerät (**20**) bei jeder durch Verschlüsselung geschützten Informationsübertragung zusammengestellt werden.

Es folgen 2 Blatt Zeichnungen

**Anhängende Zeichnungen**

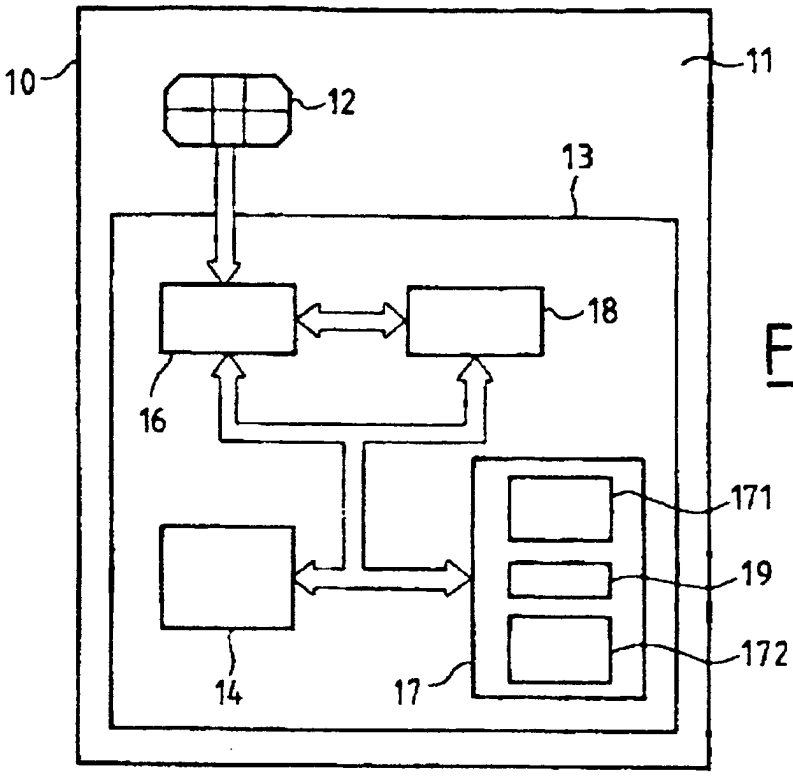


FIG_1

FIG_2

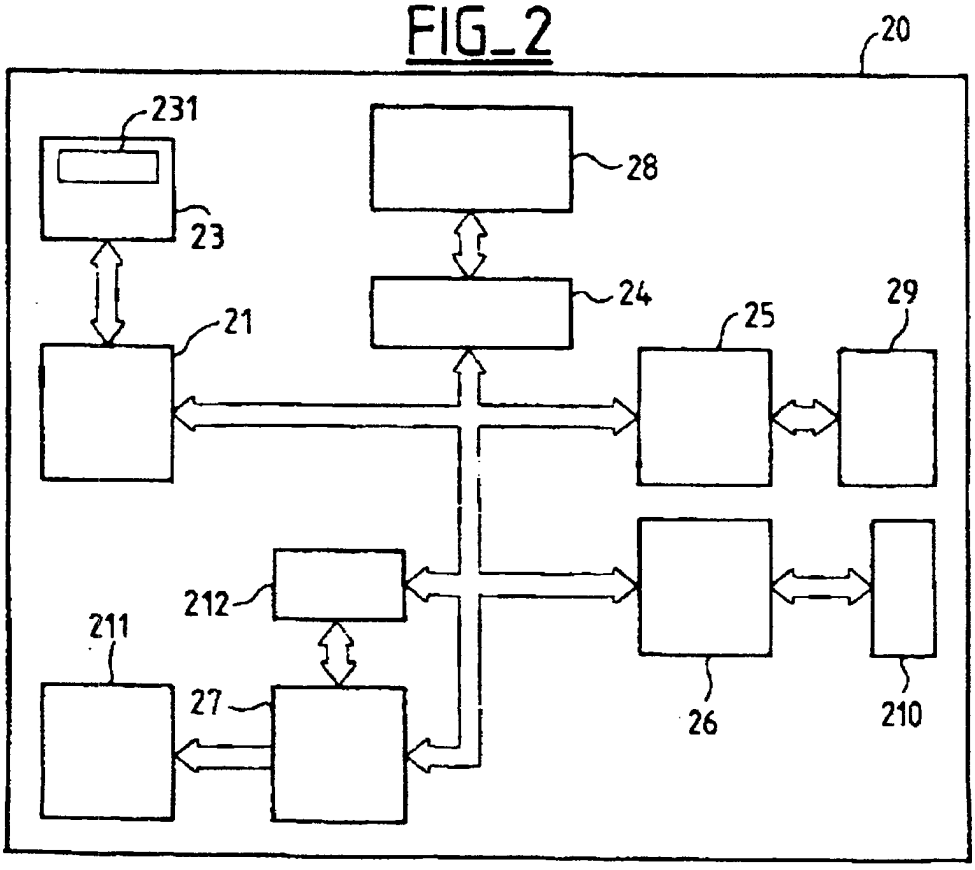

FIG_3

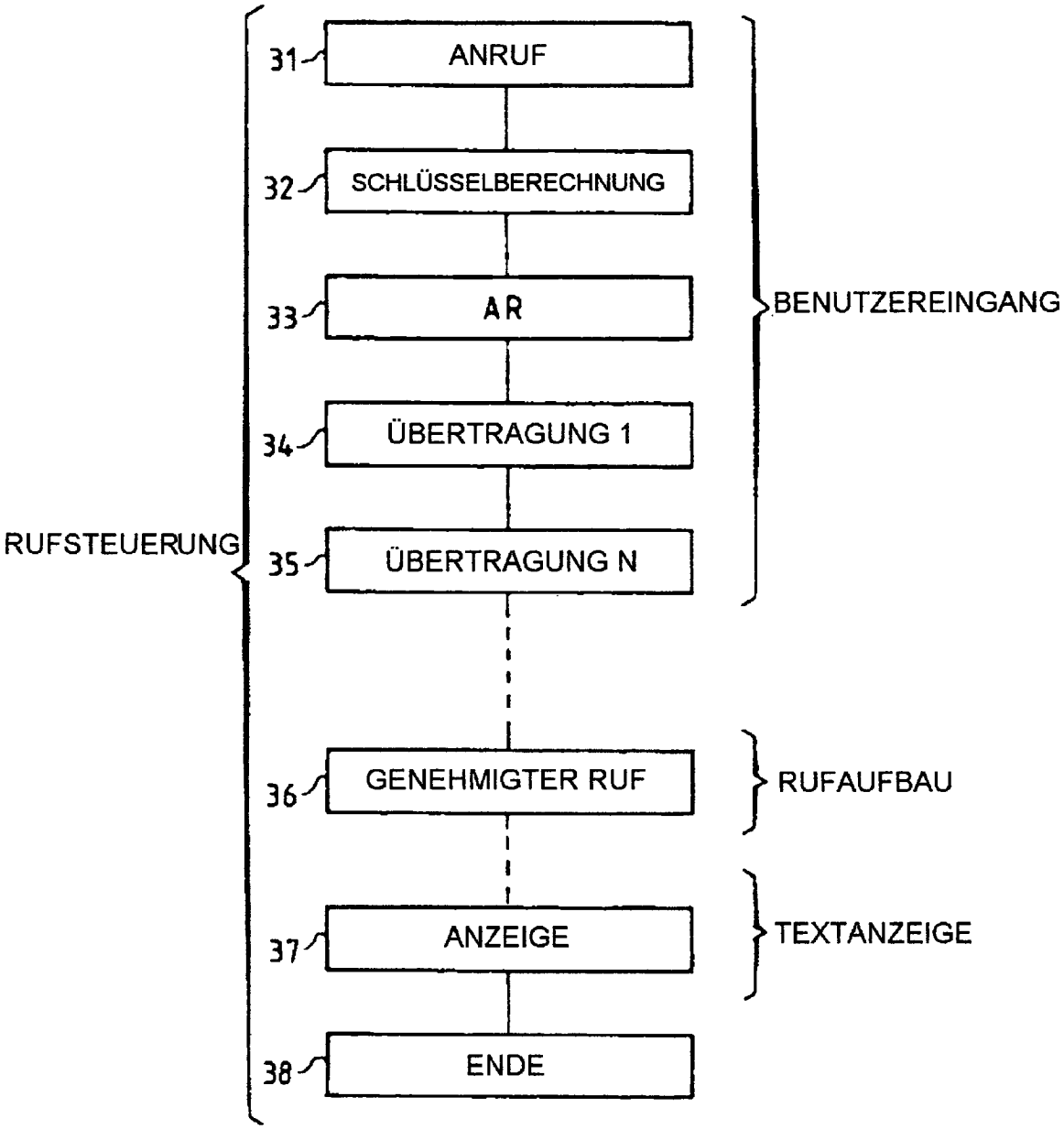


FIG_4


FIG_5