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

(10) **DE 697 36 065 T2** 2007.01.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 923 842 B1**
(21) Deutsches Aktenzeichen: **697 36 065.2**
(86) PCT-Aktenzeichen: **PCT/US97/15311**
(96) Europäisches Aktenzeichen: **97 939 691.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 1998/010611**
(86) PCT-Anmeldetag: **05.09.1997**
(87) Veröffentlichungstag der PCT-Anmeldung: **12.03.1998**
(97) Erstveröffentlichung durch das EPA: **23.06.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **07.06.2006**
(47) Veröffentlichungstag im Patentblatt: **04.01.2007**

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

(30) Unionspriorität:
706574 **05.09.1996** **US**

(84) Benannte Vertragsstaaten:
BE, DE, DK, ES, FI, FR, GB, GR, IT, SE

(73) Patentinhaber:
Ericsson Inc., Plano, Tex., US

(72) Erfinder:
OSBORN, R., William, Cary Wake, NC 27513, US

(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(54) Bezeichnung: **SYSTEM ZUM VERHINDERN VON VERFÄLSCHUNG EINES ELEKTRONISCHEN SPEICHERS**

Beschreibung

HINTERGRUND

[0001] Die Erfindung bezieht sich auf ein System zum Verhindern der Manipulation von elektronischen Speichern, und im genaueren auf Methoden und Vorrichtungen zum Verhindern von nichtautorisierter Manipulation von sicher gewünschten Speicherinhalten in einer elektronischen Vorrichtung.

[0002] Die hier offenbarte Erfindung bezieht sich auf alle elektronischen Vorrichtungen, deren Speicherinhalte in einem sicheren und vorzugsweise unveränderten Zustand aufrechterhalten werden sollen. Solch eine Anforderung kann aus Sicherheitsgründen, so wie das Verhindern von betrügerischer Manipulation des Funktelefonspeichers, erforderlich sein, oder für die Zwecke der Aufrechterhaltung der Integrität des Betriebs der elektronischen Vorrichtung in kritischen Anwendungen, so wie Flugsystemsteuerung oder Betrieb von medizinischen Instrumenten. Wie hier offenbart und beschrieben werden exemplarische Aspekte der Erfindung dargelegt in dem Kontext eines Systems und Verfahrens zum Sichern eines oder mehrerer elektronicher Speicher innerhalb eines Funktelefons. Auch wird hier ein System beschrieben, das Zugang zu und Manipulation von einem oder mehreren elektronischen Speichern in einer elektronischer Vorrichtung durch Verwendung einer Datenübertragungsvorrichtung ermöglicht, die einen Authentisierungsprozess durchläuft, bevor dieser gestattet wird, auf den elektronischen Speicher zuzugreifen. Das letztere System wird auch im Zusammenhang einer Funktelefonanwendung beschrieben. Obwohl exemplarische Ausführungsformen der offenbarten Erfindung hier im Zusammenhang mit einem sicheren Funktelefonspeicher und einem Mittel zum sicheren Zugreifen und Ändern von Speicherinhalten in Funktelefonen beschrieben sind, ist es vom Fachmann leicht zu verstehen, das Systeme in Übereinstimmung mit der Erfindung auf alle elektronischen Systeme angewendet werden können, die einen oder mehrere Speicher aufweisen, deren Inhalte unverändert bleiben sollen, oder auf deren Speicher lediglich durch autorisierte Mittel zugegriffen werden soll. Demzufolge soll der Bereich der Erfindung nicht limitiert sein durch die hier dargelegten exemplarischen Ausführungsformen, sondern stattdessen durch die hier angefügten Ansprüche und deren Äquivalente.

[0003] In den Vereinigten Staaten wurden die Verluste aufgrund von Funktelefonbetrug auf 600 Millionen Dollar im Jahr 1995 hochgerechnet. Als Reaktion darauf haben Hersteller, Dienstbereitsteller, die Föderale-Kommunikations-Kommission (FCC, Englisch: Federal Communications Commission) und Industriehandelsgruppen einer Reihe von Techniken zur Bekämpfung solchen Betrugs untersucht. Eine Mehrheit des Funktelefonbetrugs, der in den U.S. begangen wird, beinhaltet eine Form der Speichermanipulation, um die elektronische Seriennummer (ESN, Englisch: Electronic Serial Number) des Funktelefons zu verändern, die ein Funktelefon bereitstellen muss, um Kommunikationen aufzubauen. Demzufolge ist eine Betrugsprävention und Technik unter Berücksichtigung einer Regel durch die FCC, das von den Funktelefonherstellern verlangt wird, alle Mikroprozessorcodes und die ESN unveränderlich zu gestalten. Einige Hindergründe der Grundlagen von Funkkommunikationen wird unten bereitgestellt, um bei der Darstellung der Funktelekommunikationsbetriebsumgebung und verbundenen Problemen zu assistieren, die adressiert sind durch Systeme, die die vorliegende Erfindung beinhalten.

[0004] Ein vereinfachter Aufbau eines Funkkommunikationssystems ist in Fig. 1 dargestellt. Mobile Telefone M1–M10 kommunizieren mit dem festen Teil eines öffentlich geschalteten Netzwerks durch Übertragung von Radiosignalen zu und Empfang von Radiosignalen von Funkbasisstationen B1–B10. Die Funkbasisstationen B1–B10 sind wiederum mit dem öffentlich geschalteten Netzwerk über ein Mobil-Schalt-Center (MSC, Englisch: Mobile Switching Center) verbunden. Jede Basisstation B1–B10 überträgt Signale innerhalb eines korrespondierenden Bereichs oder „Zelle" C1–C10. Wie in Fig. 1 dargestellt, ist eine idealisierte Anordnung von Basisstationen so angeordnet, dass die Zellen im wesentlichen eine Fläche mit einem minimalen Betrag von Überlappung abdecken, in der mobile Telefonkommunikation normalerweise auftritt (z. B. ein Ballungsgebiet).

[0005] Wenn ein Anwender ein mobiles Telefon innerhalb einer Zelle aktiviert, überträgt das mobile Telefon ein Signal, das die Anwesenheit des mobilen Telefons der Basisstation der Zelle anzeigt. Das mobile Telefon überträgt das Signal, das dessen ESN enthalten kann, in einen designierten Konfigurationskanal, der fortwährend durch jede Basisstation überwacht wird. Wenn die Basisstation das Signal des mobilen Telefons empfängt, registriert diese die Anwesenheit des mobilen Telefons innerhalb der Zelle. Dieser Prozess kann periodisch wiederholt werden, so dass das mobile Telefon bei dem Ablauf sachgerecht registriert wird, das sich dieses in eine andere Zelle bewegt.

[0006] Wenn eine mobile Telefonnummer gewählt wird, erkennt das Zentralbüro einer Telefongesellschaft die Nummer als ein mobiles Telefon und leitet den Anruf zu einem MSC weiter. Das MSC sendet eine Funkruf-Nachricht an bestimmte Basisstationen basierend auf der gewählten mobilen Telefonnummer und aktuellen Registrierungsinformationen. Eine oder mehrere der Basisstationen überträgt eine Seite auf dessen Konfigurationskanal. Das angewählte mobile Telefon erkennt dessen Identifikation auf dem

Konfigurationskanal und antwortet auf die Seite der Basisstation. Das mobile Telefon folgt auch einem Befehl, sich auf einen angewiesenen Sprachkanal einzustellen und dann das Klingeln zu initiieren. Wenn ein mobiler Anwender eine Kommunikation beendet, wird ein signalisierender Ton an die Basisstation übertragen, und beide Seiten geben den Sprachkanal frei.

[0007] In dem zuvor beschriebenen Betrieb sind mobile Telefone nicht permanent mit einem festen Netzwerk verbunden, sondern kommunizieren über eine sogenannte „Luft-Schnittstelle" mit einer Basisstation. Diese stellt natürlich die Flexibilität eines Funkkommunikationssystems bereit, da ein Anwender einfach ein mobiles Telefon transportieren kann, ohne die Beschränkung, physikalisch mit einem Kommunikationssystem verbunden zu sein. Diese Eigenschaft erzeugt jedoch Schwierigkeiten hinsichtlich der Sicherheitsinformationen, die über Funktelefonsysteme übertragen werden.

[0008] Beispielsweise kann in einem gewöhnlich verdrahteten Telefonsystem eine zentrale Durchgangsvermittlungsstelle einen speziellen Teilnehmer identifizieren, der für die Verwendung einer Telefoneinstellung durch die Kommunikationsleitung berechnet werden soll, an dem diese physikalisch angeschlossen ist. Daher benötigt die betrügerische Verwendung des Kontos eines Teilnehmers typischerweise, dass eine physikalische Verbindung zu der Leitung des Teilnehmers gemacht wird. Dies stellt ein Entdeckungsrisiko für einen potentiellen betrügerischen Anwender dar.

[0009] Funktelekommunikationssysteme werfen andererseits nicht solche Verbindungsprobleme für den potentiellen betrügerischen Anwender auf, da diese Systeme über eine Luft-Schnittstelle kommunizieren. Ohne Sicherungsschemata können betrügerische Anwender das Konto eines anderen Teilnehmers verwenden durch Zugang zu der elektronischen Seriennummer (ESN) des Teilnehmers, die von dem mobilen Telefon an das Netzwerk zu unterschiedlichen Zeiten übertragen wird, um Kommunikationen einzurichten und aufrechtzuerhalten.

[0010] Zum Einrichten einer Standard-Funkverbindung werden zwei Identifizierungscodes durch ein mobiles Telefon zum System übertragen. Diese sind die Mobil-Identifizierungs-Nummer (MIN) und die ESN. Die MIN identifiziert einen Teilnehmer, während die ESN die aktuelle Hardware identifiziert, die durch den Teilnehmer verwendet wird. Demzufolge wird erwartet, dass die MIN, die mit einer speziellen ESN korrespondiert, aufgrund des Erwerbs neuer Ausstattung des Betreibers sich mit der Zeit ändern kann. Die MIN ist eine 34-Bit binäre Nummer, die von einer 10-stelligen Verzeichnis-Telefonnummer abgeleitet wird, während die ESN eine 32-Bit binäre Nummer ist, die eindeutig ein Mobiltelefon identifiziert. Die ESN wird typischerweise durch den Mobiltelefonhersteller eingestellt.

[0011] Ein konventionelles Authentifizierungsverfahren verwendet bei der Einrichtung von Kommunikationen beispielsweise das fortgeschrittene Mobil-Telefon-System (AMPS, Englisch: Advanced Mobile Phone System), das durch ein Flussdiagramm in Fig. 2 dargestellt ist. Gemäß diesem Verfahren empfängt eine Basisstation sowohl eine ESN als auch eine MIN von dem mobilen Telefon bei Block **200**. Diese Identifizierungscodes werden als ESN_m und MIN_m bezeichnet, um anzuzeigen, dass diese von dem mobilen Telefon empfangen werden. Als nächstes empfängt bei Block **202** die Basisstation eine ESN_{sys}, die mit MIN_m eines Systemspeichers korrespondiert. ESN_{sys} wird mit ESN_m bei Block **204** verglichen. Wenn die zwei Seriennummern die gleichen sind, fährt der Fluss zu Block **206** weiter und der Systemzugang wird erlaubt. Andernfalls wird der Systemzugang bei Block **208** untersagt.

[0012] Ein Nachteil dieses Systems ist, dass es für einen betrügerischen Anwender relativ einfach ist, gültige MIN/ESN-Kombinationen anzupassen durch Abhören der Luft-Schnittstelle oder durch andere Quellen. Da Zugänge gemäß diesem konventionellen Systems als gültig angenommen werden, wenn die MIN und ESN, die von dem mobilen Telefon empfangen wurde mit denen im Systemspeicher gespeicherten übereinstimmen, können alle notwendigen Informationen für einen betrügerischen Zugang durch elektronisches Abhören erhalten werden.

[0013] Andere Techniken zum Verhindern von betrügerischer Verwendung wurden vorgeschlagen. Zum Beispiel beschreibt U.S. Patent Nummer 5,386,486, ein Verfahren zum Registrieren einer Identifizierungsnummer in einem persönlichen Kommunikationsendgerät mit einem Dienstbetreiber. EP 0 583 100 A1 beschreibt ein Nummernzuordnungsmodul-Einstellungssystem für ein tragbares Telefon, in dem illegale Einstellungen eines Nummernzuordnungsmoduls in einem tragbaren Telefon verhindert wird.

[0014] In Systemen, die unter dem Europäischen GSM-Standard (Global System for Mobile Communication), dem Amerikanischen TIA/EIA/IS-136 Standard und dem Japanischen Personal Digital Cellular Standard Funkkommunikationssysteme betrieben werden, wird Betrug durch Abhören verhindert durch Verwendung eines Aufgabe-Antwort-Verfahrens. Gemäß dem Aufgabe-Antwort-Verfahren ist jedes mobile Telefon mit einem eindeutigen Geheimschlüssel verbunden, der sowohl in dem mobilen Telefon als auch in einer Datenbank in dem Netzwerk gespeichert ist. Ein für das System eindeutiger Algorithmus ist sowohl im mobilen Telefon als auch in gewünsch-

ten Netzwerkknoten gespeichert. Wenn ein Anruf aufgebaut wird, wird eine Authentifizierung verlangt, wobei das Netzwerk eine Aufgabe (Zufallszahl) an das mobile Telefon sendet. Basierend auf der empfangenen Aufgabe und dem gespeicherten Geheimschlüssel berechnet das mobile Telefon eine Antwort unter Verwendung des Algorithmus und überträgt die Antwort an das Netzwerk. Gleichzeitig berechnet das Netzwerk eine „erwartete" Antwort basierend auf derselben Aufgabe und dem im Netzwerk gespeicherten Geheimschlüssel. Das Netzwerk empfängt dann die durch das mobile Telefon berechnete Antwort und vergleicht die durch das mobile Telefon berechnete Antwort mit der durch das Netzwerk berechneten Antwort. Wenn eine Fehlanpassung auftritt, werden geeignete Maßnahmen ergriffen, z. B. wird der Zugang verweigert oder es wird ein Warn-Flag gesetzt. Ein Verfahren zum Ausführen einer Authentifizierungsüberprüfung zwischen einer Basisstation und einem mobilen Telefon in einem mobilen Funksystem wird im U.S. Patent Nummer 5,282,250 von P. Dent et. al. dargestellt.

[0015] In einem konventionellen analogen System wie dem AMPS wird ein Großteil des Betrugs durch betrügerische Anwender begangen, die gültige Teilnehmer „klonen" durch Akquirierung gültiger MIN/ESN-Paare und Verwendung der Paare um ein Funktelefon neu zu programmieren. In weiterentwickelten Klon-Anordnungen wird die Software eines Funktelefons neu programmiert, so dass dieses verschiedene MIN/ESN-Paare verwenden kann, was in der Praxis „Taumeln" genannt wird. Ein Funktelefon, das mit einer Taumelroutine programmiert ist, blättert durch die MIN/ESN-Paare und wählt ein MIN/ESN-Paar aus, um einen Anruf zu initiieren. Wenn der Betrug durch den Dienstanbieter oder Teilnehmer identifiziert ist, werden die MIN/ESN-Paare annulliert. Wenn beim Versuch eines Anrufs auf ein ungültiges MIN/ESN-Paar gestoßen wird, löscht die Taumelroutine einfach das MIN/ESN-Paar und fährt mit dem Blättern fort, bis ein gültiges MIN/ESN-Paar gefunden ist. Nachdem alle MIN/ESN-Paare, die in dem Funktelefon programmiert sind, annulliert sind, kehrt der Telefonanwender typischerweise zum Kloner zurück, um einen neuen Satz von MIN/ESN-Paaren in das Funktelefon einprogrammieren zu lassen.

[0016] Die meisten Funkbetrüge beinhalten einen gewissen Grad von Speichermanipulation. Dies wird mit Bezug auf **Fig. 3** beschrieben, das ein Blockdiagramm eines konventionellen Telefonspeichers und eine Prozessoranordnung darstellt. Eine Steuereinheit **300** kommuniziert mit einem ROM oder Flash-Programmspeicher **320**, einem EEPROM **310** und einem Direktzugriffsspeicher (RAM **330**) unter Verwendung des Speicherbusses **308**. Der Programmspeicher **320** ist ein permanenter Lese/Schreib-Speicher der verwendet wird, um die Mehrheit der Codes zu speichern, die für den allgemeinen Betrieb des Funktelefons verwendet werden. Der EEPROM **310** wird verwendet, um die MIN/ESN-Paare **314** und **316** zu speichern, und die Anwender-Profil-Information **312** (z. B. Schnellwählnummern) und der RAM werden zum Lesen/Schreiben des Zwischenspeichers verwendet. Es ist bekannt, dass Kloner Nachrichten zwischen den Speichern und der Steuereinheit **300** überwachen, um Informationen zu sammeln, die verwendet werden zum Umgehen oder Modifizieren von Informationen, die in dem Flashspeicher **320** oder dem EEPROM **310** gespeichert sind.

[0017] Das am meisten verbreitete Verfahren des Telefonbetrugs war die unerlaubte Verwendung von Testbefehlen, die für Telefondienste und Reparatur vorgesehen sind, um die ESN zu ändern. Jedoch sind die meisten kürzlich produzierten Telefone resistent gegenüber einer solchen Verfälschung und haben wirksam diese Attacken eliminiert. Folglich haben sich die Kloner auf weiterentwickelte Angriffsmoden verlegt.

[0018] Eine solche Technik umfasst das Entfernen des originalen EEPROM **310**, der die ESN **314** enthält, und dessen Austausch. Nach dem Entfernen wird der EEPROM studiert, um dessen Inhalte zu entschlüsseln. Die entschlüsselten Inhalte werden dann verwendet, um einen Austausch EEPROM mit einem widerrechtlich angeeigneten ESN/MIN-Paar von einem gültigen Anwenderkonto zu programmieren. Diese Technik kann für einen Kloner attraktiv sein, wenn er oder sie lediglich eine ESN zu einer Zeit verändern will. Jedoch ist diese Technik laborintensiv und nicht so qualifizierte Kloner können gedruckte Schaltungen beschädigen, wenn diese nicht extrem vorsichtig sind.

[0019] Ein großer Schritt in der Klon-Gewandtheit bezieht das Analysieren eines Mikroprozessorcodes eines Telefons und das Neuschreiben eines oder mehrerer Abschnitte des Codes ein, um eine betrügerische Identität (ESN/MIN-Paar) an eine Funkbasisstation zu übertragen. Dies bezieht häufig Nachbau-Abschnitte des Telefonhardwaredesigns ein und setzt signifikantes Verständnis des eingebetteten Softwaredesigns voraus. Der offensichtliche Vorteil dieses Verfahrens ist jedoch, dass sobald die Modifikation einmal komplett ist, das Telefon sooft gewünscht mit einer Identität neu programmiert werden kann.

[0020] Die am meisten entwickelten Angriffe kombinieren Veränderungen des Mikroprozessorcodes des Funktelefons wie oben beschrieben in Kombination mit Hardwaremodifikation. Ein Beispiel dieser Technik verwendet einen so genannten „Schattenspeicher", um die Detektierung durch konventionelle Speicherprüfroutinen zu verhindern, die lediglich während des Hochfahrprozesses ausgeführt werden,

wenn das Funktelefon das erste Mal angeschaltet wird. Der Hochfahrprozess wird gemäß einem kleinen Abschnitt des Startcodes **304** ausgeführt, der in der Steuereinheit **300** enthalten ist (siehe Fig. 3). Der Hochfahrprozess konfiguriert das Funktelefon in einen Betriebszustand und setzt einen Programmzähler in den Mikroprozessor **301** auf eine geeignete Position in dem Flashspeicher **320**. Wenn der Prozess komplett ist, kann die Steuereinheit **300** eine LED **318** erleuchten (oder ein anderes äquivalentes Signal), das dem Anwender anzeigt, dass das Telefon in Betrieb ist. Ein Kloner kann eine Verbindung **306** zwischen der Steuereinheit **300** und der LED **318** überwachen, um die Ausführung des normalen Betriebscodes in dem Flashspeicher **320** zu untergraben, wie detaillierter später beschrieben wird.

[0021] Der in einem modernen Funktelefon enthaltene Flashspeicher **320** weist eine adressierbare Kapazität von 512 K auf. Ein Kloner kann den Flashspeicher **320** entfernen und diesen mit einem 1024 K Schattenspeicher **322** ersetzen, nachdem die Inhalte des originalen Flashspeichers **320** in die ersten 512 K der 1024 K Schattenspeicher **322** kopiert wurden. Während des Hochfahrens werden alle Zugriffe auf den Programmspeicher erfolgreich in die ersten 512 K des Flashspeichers **320** geleitet. Der Kloner kann dann ein Signal überwachen, das im Telefon verfügbar ist, das anzeigt, dass der Startprozess beendet ist (so wie das LED Signal **306**), um alle zukünftigen Programmspeicherzugriffe auf den Schattenspeicher **322** zu schalten. Danach arbeitet das Funktelefon in Übereinstimmung mit Instruktionen, die im Schattenspeicher **322** zu finden sind, dessen Speicher programmiert werden kann, einen Taumelroutinencode und korrespondierende MIN/ESN-Paare zu enthalten.

[0022] Es wurden verschiedene Ansätze unternommen, um Speicherverfälschung zu verhindern. Beispielsweise beschreibt WO 91/09484 eine Sicherheitstechnik, in der Zugang zu Speichergebieten in einem mobilen Telefon lediglich durch CPU-Instruktionen erlaubt sind, die von einem ROM abgerufen werden. FR 2 681 965 beschreibt ein System zum Schützen eines Speichers dagegen beschrieben zu werden beim Auftauchen von bestimmten Ereignissen. Andere Systeme zum Verhindern von betrügerischer Verwendung und/oder Verfälschung sind im U.S. Patent Nummer 5,046,082 beschrieben, das ein Fernzugriffssystem für Funktelefone beschreibt, das nicht autorisierten Zugang und Verfälschung verhindert mit Funktelefonprogrammierung, und Nummer 5,442,645, das die Überprüfung der Integrität eines Programms oder Daten beschreibt, in denen eine Signatur durch die Prozessschaltkreise eines tragbaren Objekts berechnet wird, mit einer originalen Nachrichtensignatur verglichen wird.

[0023] Da der meiste Funkbetrug zu einem bestimmten Grad auf Speichermanipulation basiert, wägt die föderale Kommunikationskommission (FCC) momentan eine Lösung ab, die auf diesen Aspekt eines Funktelefonbetrugs gerichtet ist. Die Lösung ist eingebettet in eine vorgeschlagene FCC-Regel, die als § 22.219 bezeichnet ist. Wie gerade beschrieben verbietet § 22.919, das die Betriebssoftware eines mobilen Telefons veränderbar ist; verlangt, dass eine ESN vom Werk eingestellt ist, nicht veränderbar, übertragbar, entfernbar oder in irgendeiner Weise manipulierbar ist; und verlangt, dass der mobile Überträger inoperabel wird, wenn irgendeine Partei beinhaltend einen Hersteller versucht, die ESN, die Systemlogik oder die Firmware des Funktelefons zu entfernen oder zu verfälschen.

[0024] Vom Standpunkt eines Verbrauchers macht es die momentane Fähigkeit einfach, das ein Hersteller oder dessen herstellungsautorisierter Servicerepräsentant die Funktelefone programmieren kann, die Funktelefone zu ersetzen, die nicht einwandfrei funktionieren. Wenn beispielsweise das Funktelefon eines Teilnehmers nicht einwandfrei funktioniert, kann der Teilnehmer eine neue Einheit von einem betriebsautorisierten Repräsentanten erhalten und kann dieses programmieren lassen, um dieselbe elektronische „Persönlichkeit" der alten Einheit zu enthalten. Die elektronische Persönlichkeit eines Funktelefons beinhaltet nicht lediglich die ESN sondern auch das Nutzerprofil und einen erheblichen Betrag von Informationen, die durch den Teilnehmer in die Einheit programmiert wurden, so wie persönliche und/oder geschäftliche Telefonnummern. Reparatur/Ersatzprogramme und Technologie zum schnellen und einfachen Ändern der ESN und anderer Speicher von Funktelefonen wurden entwickelt mit der Insistenz von Funkdienstanbietern, die nicht wollen, dass deren Teilnehmer von defekten Endgeräten belästigt werden.

[0025] Unter FCC § 22.919 ist ein Teilnehmer in der oben beschriebenen Situation noch immer in der Lage, eine neue mobile Einheit zu erhalten, wenn deren alte Einheit defekt ist. Da jedoch eine neue feste ESN mit der neuen Einheit assoziiert sein wird, muss die neue ESN-Information an den Funkbetreiber übermittelt werden, der diese in dessen Datenbasis einprogrammieren muss. Dies kann zu einer langen Zeitperiode führen, während der der Teilnehmer auf keinen Dienst zugreifen kann. Der Teilnehmer wird auch sein Funktelefon neu programmieren müssen mit allen persönlichen oder geschäftlichen Telefonnummern. Ein viel signifikanteres Problem mit § 22.919 ist der nachteilige Einfluss, den dieser auf die Fähigkeit von Funkdienstbetreibern haben wird, deren Teilnehmer mit Systemaktualisierungen durch Programmieren oder Neuprogrammieren derer Funktelefone ausgestattet werden sollen.

[0026] Der praktische Einfluss, den § 22.919 auf die

Fähigkeit der Funkindustrie haben kann, die Systeme zu aktualisieren, wird im Folgenden demonstriert. Die Verwendung eines wie spezifizierten digitalen Störungskanals, z. B. in dem TIA/EIA/IS-136 Standard, ermöglicht Funkbetreiber neue erweiterte Dienste anzubieten, so wie einen Kurzmitteilungsdienst. Wenn Betreibern, Herstellern, oder autorisierten Vermittlern erlaubt wird, Änderungen an der Software und/oder Firmware des Funktelefons auszuführen, können solche Dienste schnell und effektiv über Softwareaktualisierungen der Endgeräte den Teilnehmern verfügbar gemacht werden. Unter § 22.919 (in dessen aktueller Form) werden weder ein Hersteller, ein vom Hersteller autorisierter Dienstrepräsentant noch ein Funkbetreiber in der Lage sein, solche Softwareänderungen durchzuführen. Der einzige Weg, dass ein Betreiber einen Teilnehmer eine Systemverbesserung anbieten kann, wird voraussetzen, dass der Teilnehmer ein neues Funktelefon erwirbt.

[0027] Um den Einfluss von § 22.919 auf Teilnehmer als auch auf die Herstellergemeinschaft zu verbessern, erklärt die FCC, dass die Regel anwendbar sein würde auf Funktelefone, für deren Anwendungen für Initialtypakzeptanz nach dem 1. Januar 1995 angemeldet wurden. Eigentlich hat die FCC die 20 Millionen sich momentan im Betrieb befindlichen Funktelefone als auch die Millionen von Funktelefonen, die den Betrieb nach dem 1. Januar 1995 aufgenommen haben, basierend auf Anwendungen für Typakzeptanz, die vor dem 1. Januar 1995 angemeldet wurden, veraltet. Die Tatsache, dass es so viele Funkeinheiten auf dem Markt gibt, deren elektronische Information für illegale Zwecke manipuliert werden kann, suggeriert, dass § 22.919 lediglich einen sehr kleinen Einfluss auf das Betrugsproblem haben wird. Diese Einheiten, die durch illegale Verfälschung der ESNs Betrug durchführen, können durch Verwendung der Millionen von Endgeräte, die nicht Teil von § 22.919 Restriktionen sind, fortfahren.

[0028] Wie aus dem Vorgesagten ersichtlich ist, ist die Bereitstellung eines Funktelefons, das einen sicheren Speicher aufweist, höchst erwünscht. Momentan scheint es keine Lösungen zum Nachrüsten von Funktelefonen zu geben, die diese resistent für Verfälschungen machen. Weiterhin scheint es keine Verfahren oder Vorrichtungen zum Bereitstellen von Aktualisierungen für die elektronischen Speichervorrichtungen auf solch eine Weise, dass lediglich autorisierter Zugang gewährleistet ist, zu geben.

ZUSAMMENFASSUNG

[0029] Diese und andere Nachteile und Limitierungen von konventionellen Verfahren und vorgeschlagenen Lösungen zum Verhindern der Verfälschung von Funktelefonspeichern und elektronischen Speicherverfälschung im Allgemeinen werden durch die vorliegende Erfindung überwunden, beispielsweise durch Ausführungsformen, die elektronische Speicherinhalte vor nicht autorisiertem Zugang und Manipulation schützen.

[0030] Das grundlegende Konzept der Erfindung wird durch die unabhängigen Ansprüche beschrieben. Vorteilhafte Ausführungsformen sind in den abhängigen Ansprüchen beschrieben. In Übereinstimmung mit einem Beispiel der Erfindung wird Sicherheit erreicht durch periodische Überprüfung von elektronischen Speicherinhalten in einer elektronischen Vorrichtung, um zu gewährleisten, dass die Inhalte nicht verfälscht wurden. Die Überprüfung beinhaltet die Ausführung einer Hash-Berechnung von ausgewählten Inhalten des elektronischen Speichers, um einen Prüf-Hash-Wert oder eine Prüfsignatur solcher Inhalte abzuleiten. Der Prüf-Hash-Wert wird mit einem gültigen Hash-Wert verglichen, der zuvor von glaubwürdigen Speicherinhalten abgeleitet wurde. Der gültige Hash-Wert wird vorzugsweise in einer verschlüsselten Form innerhalb des elektronischen Speichers gespeichert und lediglich für Vergleichszwecke entschlüsselt. Eine Ungleichheit zwischen dem Prüf-Hash-Wert und dem gültigen Hash-Wert zeigt eine Verfälschung des Speichers an, woraus abgeleitet wird, das eine elektronische Vorrichtung, die den elektronischen Speicher beinhaltet, als unbrauchbar betrachtet wird.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0031] Die vorangegangenen und andere Ziele, Eigenschaften und Vorteile der vorliegenden Erfindung werden einfacher verstanden durch Lesen dieser Beschreibung in Verbindung mit den Zeichnungen, in denen:

[0032] Fig. 1 ein idealisiertes Layout eines Funkkommunikationssystems darstellt;

[0033] Fig. 2 ein Flussdiagramm darstellt, das ein konventionelles Funkauthentifizierungsverfahren zur Einrichtung eines Funkanrufs darstellt;

[0034] Fig. 3 einen konventionellen Funktelefonprozessor und Speicheranordnung darstellt;

[0035] Fig. 4 einen Funktelefonprozessor und Speicheranordnung in Übereinstimmung mit einer exemplarischen Ausführungsform der Erfindung darstellt;

[0036] Fig. 5 ein Flussdiagramm darstellt, das einen exemplarischen Inbetriebnahmeprozess eines Funktelefons in Übereinstimmung mit einer Ausführungsform der Erfindung darstellt;

[0037] Fig. 6 ein Flussdiagramm darstellt, das einen exemplarischen periodischen Speicherprüfprozess in Übereinstimmung mit der Erfindung darstellt;

[0038] Fig. 7 eine exemplarische Datenübertragungsvorrichtung in Übereinstimmung mit einer Ausführungsform der Erfindung darstellt;

[0039] Fig. 8 ein Flussdiagramm darstellt, das einen exemplarischen Prozess zur Authentifizierung der Datenübertragungsvorrichtung in Übereinstimmung mit einer Ausführungsform der Erfindung darstellt;

[0040] Fig. 9 ein Flussdiagramm darstellt, das einen exemplarischen Prozess zum Eingeben einer anfänglichen ESN in einen Funkspeicher in Übereinstimmung mit einer Ausführungsform der Erfindung darstellt;

[0041] Fig. 10 ein Flussdiagramm darstellt, dass einen exemplarischen Prozess zum Neuprogrammieren einer etablierten ESN in Übereinstimmung mit der Erfindung darstellt; und

[0042] Fig. 11 eine geschützte Speicheranordnung in Übereinstimmung mit einer exemplarischen Ausführungsform der Erfindung darstellt; und

[0043] Fig. 12 ein exemplarisches Funktelefon-Programmiergerät in Übereinstimmung mit einer Ausführungsform der Erfindung darstellt.

DETAILLIERTE BESCHREIBUNG

[0044] Ein exemplarischer elektronischer Speicher, der Vorrichtungen und Verfahren in Übereinstimmung mit der Erfindung umfasst, ist unten in Zusammenhang mit einer Funktelefonanwendung offenbart. Die unten beschriebenen Beispiele sind lediglich bereitgestellt, um eine ideale Anwendung darzustellen, die die Erfindung einbettet.

[0045] Bezugnehmend auf Fig. 4 steuert eine Steuereinheit **400** den Betrieb eines Funktelefons (siehe z. B. Bezugszeichen **1204** in Fig. 12). Die Steuereinheit **400** arbeitet in Verbindung mit einem Flash-Programmspeicher **420**, einen elektronisch löschbaren programmierbaren Festwertspeicher (EEPROM) **410** und einem Direktzugriffsspeicher (RAM) **408**. Die Steuereinheit **400** beinhaltet einen Mikroprozessor **402** und einen internen Festwertspeicher (IROM) **403**. Der IROM **403** beinhaltet einen Startcode **404**, Hashing-Code **405**, Authentifizierungscode **409** und einen öffentlichen Verschlüsselungsschlüssel **406**. Die Steuereinheit **400** beinhaltet auch einen geschützten statischen Direktzugriffsspeicher (PSRAM) **407**, eine Interrupt-Steuereinheit **421** und Hardware basierte Zeitgeber **401** zum initiieren von periodischen Hash-Berechnungen durch den Mikroprozessor **402** auf ausgewählte Speicherinhalte. Der EEPROM **410** enthält Anwenderprofildaten **412**, eine ESN **414**, eine MIN **416** und ein signiertes/unsigniertes gültiges Hash-Wert-Paar **418**. Instruktionscode, der mit dem allgemeinen Betrieb des Funktelefons involviert ist, ist in dem Flash-Programmspeicher **420** enthalten. Der RAM-Speicher **408** wird als ein Notizblock für Operationen verwendet, die Teil des normalen Funktelefonanrufprozesses sind. Operationen, die sensitive Daten, Hash-Wert-Berechnungen und Authentifizierungsprozesse beinhalten, werden bevorzugt in Verbindung mit dem PSRAM **407** ausgeführt. Die Steuereinheit **400** kommuniziert mit dem Flash-Programm-Speicher **420**, den RAM **408** und dem EEPROM **410** über den Speicherbus **424**.

[0046] Ein Prozess zum Telefoneinschalten und zur Speicherüberprüfung für das in Fig. 4 dargestellte System gemäß einer exemplarischen Ausführungsform der Erfindung ist in Fig. 5 dargestellt. Nachdem das Funktelefon angeschaltet ist, wird der Startcode **404** innerhalb des IROM **403** durch den Mikroprozessor **402** ausgeführt, um die Steuereinheit zu initialisieren (Block **500**). Der Hash-Code **405** der im IROM **403** enthalten ist, wird dann ausgeführt, um eine Prüf-Hash-Wert-Berechnung über ausgewählte Inhalte des Flashprogrammspeichers **420** und dem ESN-Wert **414**, der im EEPROM **410** (Block **502**) gespeichert ist, auszuführen. Die Steuereinheit authentifiziert dann das signierte gültige Hash-Wert-Paar **418**, das im EEPROM **410** (Block **504**) gespeichert ist. Dies kann die Authentifizierung des signierten gültigen Hash-Wertes miteinbeziehen durch Bearbeiten dieses mit einem öffentlichen Schlüssel **406** und dann Vergleichen des Ergebnisses mit dem nicht signierten Hash-Wert. Der authentifizierte Hash-Wert wird dann im PSRAM **407** gespeichert (Block **506**). Der bei Block **502** abgeleitete Prüf-Hash-Wert wird dann mit dem authentifizierten Hash-Wert verglichen, der bei Block **504** abgeleitet wird (Block **508**). Wenn die zwei Hash-Werte übereinstimmen, wird der Mikroprozessorprogrammzähler auf eine geeignete Position im Flashspeicher **420** gesetzt, und ein periodischer Hash-Wert-Berechnungsprozess wird aktiviert (Block **510**), wonach das Funktelefon mit dem normalen Betrieb beginnt (Block **512**). Wenn die Hash-Werte bei Block **508** nicht übereinstimmen, wird das System in eine Endlosschleife gebracht (Block **514**), oder wird auf eine andere Weise abgeschaltet. Der vorangehende Prozess hindert einen Kloner daran, entweder ein modifiziertes Programm im Flashspeicher oder eine modifizierte ESN im EEPROM **410** auszutauschen, was dazu führen würde, dass die Hash-Werte nicht übereinstimmen würden, wodurch das Telefon inoperabel werden würde.

[0047] Damit verhindert wird, dass ein Schattenspeicher **422** für den gültigen Flashspeicher **420** nach der Initiierung des normalen Betriebs ersetzt wird, ist es vorteilhaft, periodische Hash-Wert-Bearbeitung auszuführen. Während des normalen Telefonbetriebs kann die periodische Hash-Wert-Berechnung stattfinden als Reaktion auf den Ablauf eines Zeitgebers oder als Reaktion auf andere Systemer-

eignisse. In der in Fig. 4 dargestellten exemplarischen Ausführungsform wird eine periodische Hash-Berechnung in Reaktion auf den Ablauf eines Hardware basierten Zeitgebers **401** initiiert, der bedingt, dass ein nicht maskierbarer Interrupt (NMI) erzeugt wird. Ein NMI ist ein Hardware orientierter Interrupt, der nicht durch Softwareprozesse „maskiert" werden kann. Folglich kann ein Kloner keinen Schattencode konfigurieren, der dazu bestimmt ist, einen NMI zu missachten. Ein regulärer Interrupt ist auch ein Hardware-Interrupt der mit anderen regulären Interrupts von normalen Funktelefonereignissen konkurrieren muss, um Zugang zu Mikroprozessorressourcen zu erhalten. Ein regulärer Interrupt wird anerkannt und bearbeitet, wenn es der Interrupt mit der höchsten Priorität wird, der einen Dienst anfrägt.

[0048] Da eine komplette Hash-Wert-Berechnung länger dauern kann als durch einen normalen Telefonbetrieb tolerierbar ist, ist es vorzuziehen, eine Möglichkeit zum Ausführen des Prozess auf einer stückweisen Basis in mehreren Segmenten, die über eine Zeitperiode verteilt sind (z. B. einige wenige Sekunden), bereitzustellen. In Übereinstimmung mit einem anderen Aspekt einer vorteilhaften Ausführungsform rufen Hardware basierte Zeitgeber einen Zweischrittprozess auf, um ein Segment einer Hash-Wert-Berechnung auszuführen. Als erstes bewirkt ein nicht maskierbarer Interrupt (NMI), dass der Mikroprozessor sofort die Inhalte einer nächsten Flash- oder EEPROM-Speicherposition abfrägt, die für die Einlagerung in die periodische Hash-Berechnung vorgesehen ist, und im PSRAM speichert. Der NMI ist vorzugsweise eine kurze, Topprioritätsauswahl von Interrupt, der einen vernachlässigbaren Effekt auf die Mikroprozessoraufgaben verursacht, die aktiv sein können, wenn der NMI auf tritt. Dies gewährleistet, dass keine Aktionen durch Klonsoftware stattfinden können, um die Detektierung durch die Hash-Berechnung zu vermeiden. Ein zweiter Standard-Interrupt mit einer niedrigeren Priorität wird auch durch die hardwarebasierten Zeitgeber **401** erzeugt, die einen Dienst anfragen, um das aktuelle Segment der Hash-Wert-Berechnung zu beenden, basierend auf dem Speicherbit, das zuvor durch die NMI Routine erfasst wurde. Diese Aufgabe könnte aufgeschoben werden, wie für einen normalen Anrufbearbeitungsaufgabe benötigt wird, für eine vorbestimmte maximale Zeit (T), bevor die Hardwarezeitgeber verstreichen und das Telefon abschaltet. Die maximale Zeit (T) wird so ausgewählt, dass sie geeignet ist für jede zu beendende legitime Anrufbearbeitung, für das fertig zu stellende Hash-Berechnungs-Segment und auf den Anfang des Countdownzyklusses, bevor dieser verstreicht, des zurückzusetzenden Hardwarezeitgeber. Die Strategie des Verwendens von zwei Typen von Interrupts, um periodisch ein Segment der Hash-Wert-Berechnung zu beenden, vermeidet jede Verschlechterung im System, während die Absicherung des Sicherheitschecks nicht durch Klonsoftware umgangen werden kann, die sich im Schattenflashspeicher befindet.

[0049] Ein Flussdiagramm, das einen exemplarischen periodischen Hash-Wert-Berechnungsprozess in Übereinstimmung mit der Erfindung darstellt, ist in Fig. 6 dargestellt. Bezugnehmend auf die Figur werden sowohl ein NMI als auch ein regulärer Interrupt bei Block **604** erzeugt, wenn der T1 Zähler im Hardwarezeitgeber **401** verstreicht (Block **602**). Sobald der NMI die Steuerung des Mikroprozessors übernimmt (Block **602**), schaltet das System für eine kurze Zeitperiode, während der das nächste Bit im Flash- oder EEPROM Speicher das für die Hash-Berechnung benötigt wird, in den PSRAM gespeichert wird (Block **606**), die regulären Interrupts ab oder reiht diese in einer Schlange auf. Die Steuerung wird dann an die Aufgabe zurückgegeben, die ausgeführt wurde, als der NMI auftrat (Block **608**). Innerhalb einer kurzen Zeitperiode wird unter normalen Bedingungen der normale Interrupt von dem hardwarebasierten Zeitgeber **401** gepflegt (Block **610**) und ein Segment der Hash-Berechnung wird komplettiert basierend auf dem Speicherbit, das zuvor im PSRAM gespeichert wurde (Block **616**). Wenn die Hash-Wert-Berechnung noch nicht beendet wurde, werden die hardwarebasierten Zeitgeber (T1 & T2) **401** auf ihre anfänglichen Werte zurückgesetzt (Block **624**) und der normale Telefonbetrieb geht weiter (Block **600**) bis zum nächsten Ablauf des Zeitgebers T1. Wenn der Zeitgeber T2 verstreichen sollte (Block **612**), bevor das reguläre Interrupt gepflegt wird (Block **610**), wird das Telefon ausgeschaltet (Block **614**). Der vorgegebene Ablauf des Zeitgebers T2 (solange der reguläre Interrupt korrekt gepflegt wird) hindert einen Kloner daran, die periodische Hash-Berechnung abzuschalten.

[0050] Die periodische stückweise Berechnung des Hash-Wertes wird fortgeführt, bis die Prüf-Hash-Wert-Berechnung beendet ist (Block **618**). Der zuvor authentifizierte Hash-Wert wird dann vom PSRAM abgerufen und mit dem Prüf-Hash-Wert verglichen (Block **620**). Wenn es eine Übereinstimmung gibt, werden die hardwarebasierten Zeitgeber **401** zurückgesetzt (Block **624**) und das Telefon funktioniert normal weiter (Block **600**). Wenn es keine Übereinstimmung gibt, wird das System abgeschaltet (Block **622**), z. B. durch Einstellen des Mikroprozessors **402** in eine Haltebedingung.

[0051] Die ausgewählten Inhalte des Funktelefonspeichers, über die vorzugsweise die Hash-Berechnung ausgeführt wird, enthalten Inhalte von dem Flashspeicher **420** und der ESN innerhalb des EEPROM **414**. Dies hindert einen Kloner daran, sowohl den Flashspeicher oder den EEPROM physikalisch zu entfernen oder zu modifizieren und diese mit einer neu programmierten Vorrichtung zu ersetzen, die eine modifizierte ESN und/oder Programmcode ent-

hält, um den Funkbetreiber zu betrügen. Es ist vorzuziehen, dass die ausgewählten Speicherinhalte und die verwendete Hash-Wert-Berechnung das Telefon durch Modifikation oder selbst einem Bit des Speichers, das in der Hash-Wert-Berechnung enthalten ist, ausschaltet.

[0052] In Übereinstimmung mit einem Konzept, das nicht unter die momentan beanspruchte Erfindung fällt, kann ein Funktelefon auf eine sichere Weise unter Verwendung einer Datenübertragungsvorrichtung programmiert werden. Eine exemplarische Datenübertragungsvorrichtung in Übereinstimmung mit der Erfindung ist in Fig. 7 gezeigt. Die Bezugszeichen der Steuereinheit **400**, dessen Inhalte und verbundene Speicher sind identisch mit den Bezugszeichen aus Fig. 4. Die exemplarische Datenübertragungsvorrichtung **750** beinhaltet einen sicheren Mikroprozessor **752**, der einen privaten Verschlüsselungsschlüssel **754** enthält, der mit einem öffentlichen Verschlüsselungsschlüssel **406** im IROM **403** in der Steuereinheit **400** korrespondiert. Der sichere Mikroprozessor **752** kommuniziert mit der Funktelefonsteuereinheit **400** über eine Schnittstelle **758**. Die Schnittstelle **758** kann eine verbundene serielle Verbindung, so wie eine RS-232 Verbindung, eine kabellose Infrarotschnittstelle oder eine RF-Schnittstelle, sowie die Hauptantenne eines Funktelefons (nicht dargestellt), oder einer anderen Antenne innerhalb des Funktelefons sein.

[0053] Zugang zum Funktelefonspeicher durch die Datenübertragungsvorrichtung **750** wird lediglich erlaubt, nachdem ein rigoroser Authentifizierungsprozess beendet ist. Im genaueren kann auf die Steuereinheit **400** (und verbundene Speicherkomponenten) zugegriffen werden für den Zweck des Herunterladens von Daten, nur nachdem die Datenübertragungsvorrichtung **750** einen Aufgaben-Antwort-Prozess durchlaufen hat, um dessen Authentizität zu gewährleisten. Fig. 8 stellt einen exemplarischen Prozess zum Authentifizieren der Datenübertragungsvorrichtung **750** dar. Als einen ersten Schritt (Block **800**) wird das Telefon in einen Betriebszustand gebracht, der vorzugsweise den Betrugspräventionsprozess verwendet, der zuvor mit Bezug auf Fig. 5 beschrieben wurde. Nachdem eine Schnittstelle etabliert ist, sendet der sichere Prozessor **752** eine Programmieranfragenachricht an die Steuereinheit **400** zusammen mit einer Zufallszahl (Rand1), die durch den sicheren Mikroprozessor **752** erzeugt wurde (Block **802**). Als Reaktion sendet die Steuereinheit **400** eine Zufallszahlen-Aufgabencode (Rand2) an den sicheren Mikroprozessor **752** (Block **804**). Der sichere Mikroprozessor **752** erzeugt dann eine Aufgabenantwort basierend auf Rand1, Rand2 und den privaten Schlüssel **754** (Block **806**). Die Aufgabenantwort wird durch die Steuereinheit **400** überarbeitet unter Verwendung von Rand1, Rand2 und dem öffentlichen Schlüssel **406** (Block **810**). Die bearbeitete Aufgabenantwort wird dann authentifiziert durch Vergleichen dessen Wert mit Rand2 (Block **812**). Wenn die Aufgabenantwort richtig entschlüsselt (z. B. Rand2) ist, ist die Authentizität der Datenübertragungsvorrichtung überprüft und das Telefon geht in einen Programmiermodus über (Block **814**). Danach kann die Datenübertragungsvorrichtung **750** auf die verschiedenen Speicher im Funktelefon zugreifen und/oder neue Flashspeicher **420** Inhalte herunterladen.

[0054] Wenn die Aufgabenantwort nicht gültig ist, wird ein Fehlerzähler erhöht (Block **816**). Der Fehlerzähler wird überprüft, um zu sehen, ob eine vordefinierte Anzahl (Maxcount) erreicht wurde (Block **818**). Der Fehlerzähler berücksichtigt, dass die Datenübertragungsvorrichtung **750** mit der Steuereinheit **400** über ein rauschendes Medium kommunizieren kann. Jegliche resultierende Übertragungsfehler können in einen Authentifizierungsfehler resultieren. Somit ist es vorzuziehen, dass die Datenübertragungsvorrichtung **750** mehr als eine Chance hat, das Funktelefon in einen Programmierzustand zu bringen. In einer exemplarischen Ausführungsform wurde bestimmt, dass ein Maxcount von 50 geeignet ist. Wenn die vorbestimmte Anzahl nicht erreicht wurde, wird eine Nachricht an die Datenübertragungsvorrichtung **750** gesendet, die anzeigt, dass ein Authentifizierungsfehler aufgetreten ist (Block **822**). Bei Empfang einer solchen Anzeige wird der Authentifizierungsprozess bei Block **802** neu gestartet. Wenn die vorbestimmte Anzahl von Versuchen erreicht wurde, wird das Telefon in einen ausgeschalteten Zustand gebracht, und es kann eine Nachricht angezeigt werden, die dem Nutzer anzeigt, dass das Telefon für autorisierten Dienst rückgeführt werden muss.

[0055] Nachdem die Datenübertragungsvorrichtung **750** die Neuprogrammierung aller ESN oder das Herunterladen zum Flashspeicher **420** beendet hat, initiiert die Steuereinheit **400** innerhalb des Telefons eine neue Hash-Berechnung, die beispielsweise die geänderten Inhalte des Flashspeichers **420** und die ESN **414** enthält. Der resultierende Hash-Wert wird an die Datenübertragungsvorrichtung **750** für eine digitale Signatur, die den privaten Schlüssel **754** verwendet, gesendet. Der signierte Hash-Wert wird dann zur Steuereinheit **400** zurückgegeben zum Speichern im EEPROM **410** zusammen mit einer unsignierten Version desselben Hash-Wertes.

[0056] Die ESN kann neu programmiert werden, doch aus Sicherheitsgründen wird die Neuprogrammierung der ESN vorzugsweise auf einer Werkstufe durchgeführt anstelle von autorisierten Werksrepräsentanten. Die Programmierung einer ESN kann in zwei Situationen auftauchen: Initiale ESN Programmierung während der Herstellung und Neuprogrammierung einer existierenden ESN. Eine initiale ESN kann programmiert werden unter Verwendung einer

Datenübertragungsvorrichtung, die der aus Fig. 7 ähnlich ist. Der initiale ESN Programmierprozess wird unten mit Bezug auf Fig. 9 beschrieben.

[0057] Als einen ersten Schritt (Block **900**) wird das Telefon in einen Betriebszustand gebracht (siehe Fig. 5). Der Etablierung einer Schnittstelle mit dem Telefon folgt, dass der sichere Prozessor **752** eine ESN Programmieranfragenachricht an die Steuereinheit **400** zusammen mit einer Zufallszahl (Rand1) sendet (Block **902**). Die Steuereinheit **400** führt eine Überprüfung durch, um zu bestimmen, ob die ESN innerhalb des Telefons überall Null ist, was immer der Fall ist für ein neu hergestelltes Telefon (Block **904**). Wenn die ESN nicht überall Null ist, wird die ESN Programmiermodusanfrage abgelehnt (Block **906**). Wenn die ESN überall Null ist, wird ein im wesentlichen gleich dem in Schritt **804** bis **820** aus Fig. 8 Aufgaben-Antwort-Prozess initiiert (siehe Block **908**). Der erfolgreichen Authentifizierung der Datentransfervorrichtung **750** folgt, dass eine neue ESN in den EEPROM **410** heruntergeladen werden kann.

[0058] Nachdem die Datenübertragungsvorrichtung **750** das Herunterladen der ESN in den EEPROM **410** beendet hat, initiiert die Steuereinheit **400** eine neue Hash-Berechnung, die die neue ESN **440** beinhaltet. Der resultierende Hash-Wert wird zur Datenübertragungsvorrichtung **750** für eine digitale Signatur, die den privaten Schlüssel **754** verwendet, gesendet. Der signierte Hash-Wert **480** wird dann an die Steuereinheit **400** zum Speichern im EEPROM **410** zurückgegeben zusammen mit einer nicht signierten Version desselben Hash-Wertes.

[0059] Eine existierende ESN kann auch neu programmiert werden. Der ESN Neuprogrammierungsprozess wird vorzugsweise lediglich im Werk ausgeführt und nicht durch lokale autorisierte Werksrepräsentanten. Zusätzliche Sicherheit wird bereitgestellt durch Verwendung eines Satzes von Mikroprozessorinstruktionen, die lediglich in der Fabrik verfügbar sind, die in ein Telefon zum Zweck der Veränderung einer ESN geladen werden, die zuvor in das Telefon programmiert war. Der Prozess kann ausgeführt werden unter Verwendung einer Datenübertragungsvorrichtung, die der in Fig. 7 dargestellten ähnlich ist, und unten mit Bezug auf Fig. 10 beschrieben wird.

[0060] Als ein erster Schritt (Block **1000**) wird das Telefon in einen regulären Programmiermodus gemäß mit dem in Fig. 8 dargestellten Prozess gebracht. Eine Werksdatenübertragungsvorrichtung **750** enthält ESN Neuprogrammierungscode **756**, der in den PSRAM Speicher **407** des Funktelefons heruntergeladen werden kann, um eine ESN Neuprogrammierung zu ermöglichen. Nachdem das System in den Programmiermodus gebracht wurde, wird der ESN Neuprogrammierungscode **756** in den PSRAM **407** heruntergeladen (Block **1002**). Durch Ausführen des ESN Neuprogrammierungscode **756** nullt die Steuereinheit **400** die existierende ESN (Block **1004**) und initiiert den ESN Neuprogrammierungsprozess (Block **1006**).

[0061] Nachdem die Datenübertragungsvorrichtung **750** die Eintragung der neuen ESN in den EEPROM **410** beendet hat, initiiert die Steuereinheit **400** eine neue Hash-Berechnung, die die neue ESN **414** enthält (Block **1008**). Der resultierende Hash-Wert wird zur Datenübertragungsvorrichtung **750** für eine digitale Signatur, die den privaten Schlüssel **754** verwendet, gesendet (Block **1010**). Der signierte Hash-Wert **480** wird dann zur Steuereinheit **400** zur Speicherung im EEPROM **410** zusammen mit einer nicht signierten Version desselben Hash-Wertes (Block **1012**) zurückgegeben.

[0062] Die Hash-Wert-Berechnung und die digitale Signatur in den exemplarischen Ausführungsformen der vorliegenden Erfindung werden ausgeführt unter Verwendung von Einweg Hash-Funktionen und privaten/öffentlichen Schlüsselauthentifizierungsschemata. Eine Einweg-Hash-Funktion wird verwendet, um den Hash-Wert abzuleiten, der repräsentativ für Speicherinhalte innerhalb des Funktelefons ist. Das öffentliche/private Schlüsselsystem wird verwendet zur Bereitstellung von Sicherheit für den gültigen Hash-Wert, der im EEPROM gespeichert ist, und eine Datenübertragungsvorrichtung oder einen Programmierer authentifiziert, der versucht, den Speicher im Funktelefon zu manipulieren. Einweg-Hashing ist dem Fachmann bekannt und beispielsweise im U.S. Patent Nummer 5,343,527 von Moore beschreiben.

[0063] Eine Einweg-Hash-Funktion ist eine Funktion, die in einer Vorwärtsrichtung einfach zu berechnen ist, aber schwierig in einer Rückwärtsrechnung zu berechnen ist. Eine Einweg-Hash-Funktion, H(M), bearbeitet eine beliebig lange Eingabe, M, welche exemplarische die vorliegende Erfindung ausführt, und in ausgewählten elektronischen Speicherinhalten enthalten ist. Die Hash-Funktion gibt einen Hash-Wert mit einer festen Länge zurück, h (siehe Gleichung 1).

$$h = H(M) \qquad \text{Gleichung 1}$$

[0064] Es gibt viele Funktionen, die eine Eingabe mit beliebiger Länge annehmen und eine Ausgabe mit einer festen Länge ausgeben können, jedoch haben Einweg-Hash-Funktionen die folgenden zusätzlichen Eigenschaften: gegebenes M, einfach zu berechnendes h; gegebenes h, schwer zu berechnendes M; und gegebenes M, schwer zu findende andere Nachricht, M', so dass H(M) = H(M').

[0065] Der grundlegende Angriff gegen einen Einweg-Hash ist: mit gegebenem Hash-Wert der Spei-

chereingabe (gehashte Inhalte) würde ein Kloner begehren, einen anderen Satz von Speicherinhalten, M', zu erzeugen, so dass H(M) = H(M'). Wenn der Kloner dabei erfolgreich wäre, würde dies die Sicherheit der Einweg-Hash-Funktion untergraben. Das Ziel des Einweg-Hash ist, eine eindeutige Signatur oder Fingerabdruck von M bereitzustellen. In der vorliegenden Erfindung wird eine sichere Einweg-Hash-Funktion auf ausgewählten Inhalten eines Funktelefonspeichers ausgeführt, um einen Prüf-Hash-Wert zu produzieren. Der Prüf-Hash-Wert wird mit einem gültigen Hash-Wert verglichen, der zuvor produziert wurde durch Ausführen der Einweg-Hash-Funktion auf ausgewählten Speicherinhalten des Speichers, der dafür bekannt ist, dass dieser authentisch ist.

[0066] In einer bevorzugten Ausführungsform wird ein Nachrichtenextraktalgorithmus, so wie MD5, für die sichere Einweg Hash-Berechnung verwendet. Der MD5 Algorithmus erzeugt einen N-Bit-Hash oder ein Nachrichtenextrakt der eingegebenen Nachricht (d. h., des ausgewählten Speicherinhalts). Der MD5 Algorithmus ist sehr empfindlich darin, dass eine Änderung in einem einzigen Bit der ausgewählten Inhalte statistisch darin resultiert, dass in der Hälfte der Hash-Wert-Bits Änderungen auftreten. Der MD5 Algorithmus ist bekannt für dessen Geschwindigkeit und Einfachheit. Geschwindigkeit ist ein wichtiger Gesichtspunkt, da der Zeitbedarf bei Funktelefonmikroprozessoren nicht so groß sein kann, so dass dieser nicht akzeptable Wechselwirkung bzw. Interferenz mit normalen Systemprozessen hervorruft.

[0067] Der MD5 Algorithmus ist geeignet, da dieser auf einer inkrementellen Basis ausgeführt werden kann, wodurch eine Unterbrechung des Hash-Prozesses ermöglicht wird, so dass eine gewöhnliche Mikroproessoraufgabe angesteuert werden kann, bevor das Hashing fortgesetzt wird. Darüber hinaus ist der MD5 Algorithmus gut geeignet für die Verwendung in konventionellen Mikroprozessorarchitekturen. Andere Einweg-Hash-Algorithmen, die in Übereinstimmung mit Ausführungsformen der vorliegenden Erfindung verwendet werden können, aber nicht limitiert sind auf: Snerfu, H-Hash, MD2, MD4, sicherer Hash-Algorithmus (SHA) und HAVAL. Der Fachmann ist einfach in der Lage, einen Mikroprozessor zu programmieren, um den Einweg Hash-Prozess auszuführen.

[0068] Algorithmen mit öffentlichem Schlüssel verwenden zwei Schlüssel, wovon einer öffentlich verfügbar und der andere privat (geheim) gehalten wird, für Aufgaben wie Verschlüsselung und Entschlüsselung von Nachrichten, Nachrichtenauthentifizierung und digitale Signaturen. Die Schlüssel können auf unterschiedlichen Weisen verwendet werden, um unterschiedliche Ziele zu erreichen. Wenn beispielsweise das Ziel ist, eine Nachricht geheim zu halten, sollte der private Schlüssel durch einen Empfänger geheim gehalten werden, so dass lediglich der Empfänger die Nachricht entschlüsseln kann. In einem solchen Fall kann der Verschlüsselungsschlüssel öffentlich bekannt sein und bekannt sein, dass dieser mit einem speziellen potentiellen Empfänger assoziiert ist. Obwohl dem Sender zugesichert werden kann, dass die Informationen in diesem Prozess sicher sind, kann dem Empfänger die Senderauthentizität nicht versichert werden. Wenn der private (geheime) Schlüssel des Paares des Schlüssels geheim gehalten bleibt durch einen Sender zum Verschlüsseln, kann jedem Empfänger mit einem korrespondierenden öffentlichen Schlüssel die Authentizität des Senders versichert werden, obgleich ohne eine Versicherung der Geheimhaltung. Es ist das letztere Schema, das zur Authentifizierung einer Datenübertragungsvorrichtung in Übereinstimmung mit der vorliegenden Erfindung verwendet wird.

[0069] Algorithmen mit öffentlichem Schlüssel arbeiten basierend auf mathematischen Falltür-Funktionen, die es rechnerisch unausführbar machen, den privaten Schlüssel vom öffentlichen Schlüssel abzuleiten. Im Fall des gut bekannten RSA (Rivest, Shamir, und Adleman) Algorithmus, hängt die Sicherheit von der Schwierigkeit der Fakturierung des Produkts von zwei großen Primzahlen ab. Die Schlüsselauswahl beginnt mit der Auswahl von zwei großen Primzahlen p und q, die miteinander multipliziert eine große Zahl n erzeugen.

$$n = pq \qquad \text{Gleichung 2}$$

[0070] Der Verschlüsselungsschlüssel e wird dann zufällig ausgewählt, so dass e und $(p - 1)(q - 1)$ relative Primzahlen sind. Schließlich wird Euklid's Algorithmus verwendet, um den Verschlüsselungsschlüssel d zu berechnen, so dass

$$F = (p - 1)(q - 1) \qquad \text{Gleichung 3}$$

$$Ed = 1(\text{mod}F) \qquad \text{Gleichung 4}$$

[0071] Die Zahlen e und n sind öffentliche Schlüssel; die Zahl d ist der private Schlüssel. Gleichung 5 ist der RSA Verschlüsselungsprozess, und Gleichung 6 ist der Entschlüsselungsprozess.

$$C = M^c(\text{mod } n) \qquad \text{Gleichung 5}$$

$$M = C^d(\text{mod } n) \qquad \text{Gleichung 6}$$

[0072] Ein Gegner, der in der Lage ist, n zu fakturieren, könnte Gleichung 3 verwenden, um den Teilungsrest F zu bestimmen, und dann den privaten Schlüssel d aus Gleichung 4 zu bestimmen, der den öffentlichen Schlüssel e gibt. Nichts desto trotz ist wie oben erwähnt n normalerweise so groß, so dass solches Fakturieren unpraktisch wird. Weitere Details

über den RSA Algorithmus können in U.S. Patent Nummer 4,405,829 von Rivest et al gefunden werden.

[0073] In den bevorzugten Ausführungsformen der vorliegenden Erfindung werden der Fiat-Shamir (FS) Algorithmus oder Varianten davon verwendet (es wird Bezug genommen auf das U.S. Patent Nummer 4,748,668, dessen Inhalte hier durch Bezugnahme komplett eingebettet werden). Der FS Algorithmus ist angepasst, um eine Authentifizierung und ein digitales Signaturschema zu implementieren, das gut angepasst ist an die limitierten Berechnungskapazitäten von typischen Funktelefonen.

[0074] Der FS Algorithmus unterscheidet sich von den vorherigen Schemata wie RSA darin, dass der FS Algorithmus Faktoren verwendet basierend auf der Schwierigkeit, die Inverse einer quadratischen Residuen (v_i) modulo n zu finden. Im genaueren verwendet das FS Schema das Auswählen einer Zahl n, die das Produkt von zwei großen Primzahlen ist, die vorzugsweise eine Länge zwischen 512 und 1064 Bits hat. Ein öffentlicher Schlüssel (v): v_1, v_2, ..., v_k, und privater Schlüssel (s): s_1, s_2, ... s_k, werden so erzeugt, dass s_i = sqrt(1(v_1)mod n. Die Schwierigkeit des Findens der Inverse (1/v_1)mod n innerhalb des Inhalts der vorherigen Gleichung kann gezeigt werden, dass diese äquivalent ist mit der Schwierigkeit des Findens des Faktors der Primzahl n. Ohne Sicherheit zu opfern, wird der Algorithmus viel schneller als andere Schemata ausgeführt. Tatsächlich hat sich herausgestellt, dass das FS Schema das RSA Schema übertrifft, nämlich dass die FS Berechnung lediglich 1% bis 4% der modularen Multiplikation benötigt, die normalerweise benötigt wird, um die notwendigen Authentifizierungsberechnungen durchzuführen. Dies führt dazu, dass die Authentifizierung eines signierten Hash-Wertes mit einer Geschwindigkeit ausgeführt wird, die bis zu zwei Größenordnungen schneller ist als bei der Verwendung des RSA Schemas, um die selbe Aufgabe durchzuführen. Folglich kann die Datenübertragungsvorrichtung Authentifizierung und der periodische Prüf-Hash-Wertvergleich durch Verwendung eines FS Schemas beträchtlich beschleunigt werden im Vergleich zur Verwendung eines RSA Schemas. Bei der Massenprogrammierung von Funktelefonen oder anderen elektronischen Speichern auf einer Werksstufe reduziert die Verwendung des FS Algorithmus die Produktionszeit durch schnelleres Erzeugen einer digitalen Signatur des gültigen zu speichernden Hash-Wertes. Es können auch andere Algorithmen angewendet werden, die umfassen aber nicht limitiert sind auf ELGAMAL, DSA, und Fiege-Fiat-Shamir.

[0075] In Übereinstimmung mit einem anderen System, das nicht unter die beanspruchte Erfindung fällt, hat die Steuereinheitshardware innerhalb des Funktelefons Eigenschaften, die einen Kloner davon abhalten, die Inhalte des sicheren Speichers zu bestimmen oder die zuvor beschriebenen Sicherheitsschemata zu umgehen. Fig. 11 stellt Steuereinheitshardware, externe Speicher und Details von Speicher/Adress-Bus-Struktur dar. Mit Ausnahme der Chipauswahllogik **1122** und der Sicherheitslogik **1124** sind die Funktion und der Betrieb der Elemente in der Steuereinheit dieselben wie die in Fig. 4 beschriebenen. Die Chipauswahllogik **1122** decodiert Adressen auf dem Mikroprozessor Adressbus **1102** um Hardwareauswahlsignale für Speicherkomponenten und mit dem Bus **1102** verbundenen Hardwarevorrichtungen bereitzustellen. Beispielsweise, wenn jedes Mal eine Adresse auf dem Adressbus **1102** auftaucht, der dem IROM Speicher **403** zugeordnet ist, wird eine IROM Chipauswahl (CS) aktiviert.

[0076] Die Sicherheitslogik **1124** funktioniert, um einen Zugriffsversuch auf Inhalte des PSRAM **407** zu detektieren, oder um die Hardware basierten Zeitgeber **401** zurückzusetzen, die Mikroprozessorinstruktionscode verwenden, der in einer Speichervorrichtung gespeichert ist, die ein anderer ist als der IROM **403**. Beispielsweise wird eine Lese- oder Schreib-Instruktion, die sich im Flashspeicher **420** mit einer Zieladresse einer Speicherposition im PSRAM **407** befindet, als eine illegale Operation detektiert. Jeder illegale Zugriffsversuch resultiert darin, dass der Mikroprozessor in einen Haltzustand gebracht wird, der eine komplette Energierücksetzung des Funktelefons benötigt, um zu einer normalen Operation zurückzukehren.

[0077] Die Sicherheitslogik ist eine Implementierung der folgenden Logikgleichungen:

S = ↑Supvr•B Logikgleichung 1

Halt = notS•(A + C) Logikgleichung 2

S	= Sicherheitsmodus;
↑Supvr	= Ein Übergang des Mikroprozessors in den Überwachungsmodus;
A	= Chipauswahlsignal für den PSRAM Speicher;
B	= Chipauswahlsignal für den IROM Speicher;
C	= Chipauswahlsignal für die Hardwarezeit; und;
Halt	= Eine Hardwaresteuerungseingabe an den Mikroprozessor, die diesen dazu bringt, in eine Endlosschleife oder in eine permanente Wartebindung einzutreten bis die Energie entfernt und wieder dem Telefon zugeführt ist.

[0078] Die obere Logikgleichung 1 gibt an: Der Sicherheitsmodus (S) wird eingestellt, wenn immer der Mikroprozessor in den Überwachungsmodus (↑Sup-

vr) überwechselt zur selben Zeit, in der die IROM **403** Chip-Auswahl aktiv ist (•B). Die obere Logikgleichung 2 gibt an: Die Mikroprozessor-Halt-Eingabe wird aktiviert, wenn die Steuereinheit **400** nicht dem Sicherheitsmodus (notS) ist und entweder die PSRAM **407** oder die Hardwarezeitzeitgeber-Chipauswahl aktiv sind (•(A + C)). Diese Logik verhindert wirksam die Umgehung der Sicherheitsmessungen, die durch die Hash-Wert-Vergleiche und die zuvor beschriebenen Authentifizierungsprozesse bereitgestellt werden, da legitime Zugriffe auf den PSRAM **407** und Zurücksetzungsbefehle für die Hardwarezeitgeber **401** vorzugsweise vom Code kommen, der im IROM **403** gespeichert ist.

[0079] Der gesamte legitimierte Code, der sich im IROM Speicher **406** befindet (Startcode, Hash-Code, öffentlicher Schlüsselcode und Authentifizierungscode), wird bevorzugt durch Befehle eingeklammert, die dazu führen, dass der Sicherheitsmodus eingestellt wird beim Beginn der Routine und beim Verlassen der Routine gelöscht wird. In einer bevorzugten Ausführungsform der Erfindung wird ein Software-Interrupt-Befehl (der im allgemeinen in modernen Mikroprozessoren verfügbar ist) an den Beginn von jeder Routine im IROM **403** platziert, um den Mikroprozessor **402** in einen Überwachungsmodus zu bringen, und um ein Mikroprozessor Hardwaresignal SPVR zu aktivieren. Da das IROM **403** Chipauswahlsignal zu dieser Zeit aktiv sein wird, wird der Sicherheitsmodus S eingestellt sein. Das Ausführen eines Zurückkehrbefehls am Ende der Softwareroutine bricht den Sicherheitsmodus ab.

[0080] Die Datenübertragungsvorrichtung umfasst eine vom Werk bereitgestellte Sicherheitseinheit, die in Kombination mit einem Allzweckcomputer verwendet werden kann. Eine exemplarische Anordnung ist in Fig. 12 dargestellt. Eine Sicherheitseinheit **1200** ist an den I/O-Anschluss eines PC **1202** über einen Standard-Verbinder **1206** angebracht. Ein zweiter Anschluss am PC **1202** wird in Verbindung mit einem zweiten Standard-Verbinder **1208**, so wie eine RS-232, einem Kabel oder einer Infrarotverbindung, verwendet, um mit einem Funktelefon **1204** anzukoppeln. Die in Fig. 8 dargestellten Prozesse können ausgeführt werden unter der in Fig. 12 dargestellten Anordnung, um den Funktelefon-Neuprogrammierungsprozess auszuführen. Ein autorisierter Werksdienstrepräsentant, der einen Standard-PC und eine Sicherheitseinheit **1200** hat, ist ausgestattet, um Telefone neu zu programmieren.

[0081] Ein existierendes Funktelefon kann bereitgestellt werden mit Feldprogrammfähigkeit, die sicher ist gegen Angriffe, die nicht das Erhalten von Zugriff auf interne gedruckte Schaltkreiskartenanordnungen beinhalten. Dieser Level von Schutz ist sehr wirksam gegen die meisten allgemeinen Verfahren von Klon-Angriffen, in denen Speicherinhalte innerhalb des Telefons modifiziert werden unter Verwendung von Testbefehlen, auf die über einen externen Telefonverbinder zugegriffen werden kann. Dies kann geschehen durch Aktualisieren eines aktuellen Funktelefons, um die Datenübertragungsvorrichtung (DTD, Englisch: Data Transfer Device) Authentifizierungsprozedur, die in Fig. 8 beschrieben ist, vor der Zugriffserlaubnis auf die Feldprogrammierungsbefehle zu verwenden. Sowohl der Authentifizierungssoftwarecode als auch der öffentliche Schlüssel sind im existierenden Flashspeicher gespeichert, wodurch jegliche Veränderungen von aktuellen konventionellen Designs vermieden wird.

[0082] Es wurden exemplarische Anwendungen der Erfindung im Zusammenhang mit Einweg-Hashing und Schlüsselverschlüsselungssystemen beschrieben, die beim Sichern und Programmieren eines elektronischen Speichers in Funktelefonen Anwendung finden. Jedoch erkennt der Fachmann, dass jede geeignete Funktion, Berechnung, Algorithmus, Verfahren oder System zu Ableiten einer Signatur von Speicherinhalten in Übereinstimmung mit der Erfindung angewendet werden können. Des weiteren wurde die Erfindung mit Bezug auf spezielle Ausführungsformen beschrieben. Jedoch ist es einfach ersichtlich für den Fachmann, dass die Erfindung in spezifischen anderen als den bevorzugten Ausführungsformen verkörpert werden kann. Beispielsweise ist es möglich, die Erfindung in allen elektronischen Speichern und/oder elektronischen Speicherprogrammierungs- oder Zugriffsvorrichtungen zu verkörpern. Zusätzlich kann die Erfindung ausgeführt werden in digitalen Signalprozessoren, Anwendungsspezifischen Prozessoren oder in allen anderen Prozessoren oder elektronischen speicherorientierten Systemen. Deshalb sind die hierin beschriebenen bevorzugten Ausführungsformen lediglich beschreibend und sollten nicht beschränkend verstanden werden. Der Bereich der Erfindung wird vielmehr durch die eingefügten Ansprüche gegeben als durch die vorangegangene Beschreibung.

Patentansprüche

1. Eine elektronische Vorrichtung, umfassend:
einen Speicher (**410**, **420**); gekennzeichnet durch
einen Mikroprozessor (**402**), der konfiguriert ist, um:
eine Hash-Berechnung von authentifizierten Speicherinhalten durchzuführen, um einen gültigen Hash-Wert anzufertigen;
periodisch eine Hash-Berechnung der Inhalte des Speichers (**410**, **420**) durchführen, um einen Audit-Hash-Wert abzuleiten, Authentifizieren des gültigen Hash-Wertes und Vergleichen des Audit-Hash-Wertes mit dem authentifizierten Hash-Wert, wobei eine Differenz zwischen dem Audit-Hash-Wert und dem authentifizierten Hash-wert die Veränderung des Speichers (**410**, **420**) anzeigt; und

Deaktivieren der elektronischen Vorrichtung, sobald der Audit-Hash-Wert nicht mit dem gültigen Hash-Wert übereinstimmt.

2. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum periodischen Ableiten des Hash-Wertes gemäß dem Ablauf eines Hardwarebasierten Zeitgebers umfasst.

3. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Speicher einen Flash-Speicher (**420**) und einen EEPROM (**410**) enthält.

4. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, ferner umfassend:
ein geschützter Direktzugriffsspeicher (**407**) zum Durchführen der Hash-Berechnung in Verbindung mit dem Mikroprozessor (**402**).

5. Die in Anspruch 3 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor Mittel zum Ableiten des Audit-Hash-Wertes umfasst, basierend auf ausgewählten Inhalten des Flash-Speichers (**420**) und des EEPROM (**410**).

6. Die in Anspruch 5 beanspruchte elektronische Vorrichtung, wobei die ausgewählten Inhalte eine elektronische Seriennummer enthalten.

7. Die in Anspruch 5 beanspruchte elektronische Vorrichtung, wobei die ausgewählten Inhalte Mikroprozessor-Programmcode enthalten.

8. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Authentifizieren des gültigen Hash-Wertes unter Verwendung eines öffentlichen Schlüssels, der im Speicher (**410**, **420**) gespeichert ist, umfasst.

9. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Verschlüsseln des gültigen Hash-Wertes mit einer gegebenen digitalen Signatur unter Verwendung eines privaten Schlüssels umfasst.

10. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Durchführen der Hash-Berechnung unter Verwendung einer Gruppe von Hash-Funktionen umfasst, umfassend: Snerfu, H-Hash, MD2, MD4, MD5, Sicherer Hash Algorithmus (SHA) und HAVAL.

11. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Authentifizieren und Verschlüsseln unter Verwendung eines einer Gruppe von öffentlichen/privatem Schlüssel System Algorithmen umfasst, umfassend: ELGAMAL, RSA; DAS; Fiege-Fiat-Shamir und Fiat-Shamir.

12. Die in Anspruch 4 beanspruchte elektronische Vorrichtung, ferner umfassend Sicherheitslogik zum Überwachen des Zugangs zum geschützten Direktzugriffsspeicher.

13. Die in Anspruch 1 beanspruchte elektronische Vorrichtung, wobei die elektronische Vorrichtung ein Mobiltelefon ist.

14. Die in Anspruch 5 beanspruchte elektronische Vorrichtung, wobei die Inhalte des Flash-Speichers Betriebsanweisungen für die elektronische Vorrichtung enthält, und die Inhalte des EEPROM einen gültigen Hash-Wert enthalten, und wobei der Mikroprozessor Mittel zum Ausführen einer Einweg-Hash-Berechnung über ausgewählte Abschnitte von authentifizierten Flash- und EEPROM-Inhalten umfasst, um einen gültigen Hash-Wert anzufertigen, Mittel zu periodischen Erzeugen eines Audit-Hash-Wertes durch Ausführen der Hash-Berechnung über die ausgewählten Abschnitte, und Mittel zum Vergleichen des Audit-Hash-Wertes mit dem authentifizierten Hash-Wertes zum Beurteilen, ob mindestens einer der Flash- und EEPROM-Speicher verändert wurde.

15. Die in Anspruch 14 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Durchführen einer Einweg-Hash-Berechnung unter Verwendung einer Gruppe von Hash-Funktionen umfasst, umfassend: Snerfu, H-Hash, MD2, MD4, MD5, Sicherer Hash Algorithmus (SHA) und HAVAL.

16. Die in Anspruch 9 beanspruchte elektronische Vorrichtung, wobei der Mikroprozessor (**402**) Mittel zum Verschlüsseln des gültigen Hash-Wertes mit einer digitalen Signatur durch den privaten Schlüssel unter Verwendung von zu der elektronischen Vorrichtung externen Mitteln umfasst.

17. Ein Verfahren zum Detektieren von Speicherverfälschung in einer elektronischen Vorrichtung, wobei das Verfahren dadurch gekennzeichnet ist, dass ein Mikroprozessor in der elektronischen Vorrichtung die Schritte ausführt:
Speichern eines signierten gültigen Hash-Wertes, der angefertigt wird durch Durchführen einer Hash-Berechnung auf ausgewählten Inhalten eines Speichers (**410**, **420**), deren ausgewählte Speicherinhalte authentifiziert sind;
periodisches Anfertigen eines Audit-Hash-Wertes durch periodisches Durchführen der Hash-Berechnung auf ausgewählten Inhalten des Speichers (**410**, **420**), Authentifizieren des signierten, gültigen Hash-Wertes, und Vergleichen des Audit-Hash-Wertes mit dem authentifizierten, gültigen Hash-Wert, wobei eine Differenz zwischen dem Audit und dem authentifizierten, gültigen Hash-Werten die Veränderung der ausgewählten Speicherinhalten anzeigt;

und
Deaktivieren der elektronischen Vorrichtung, wenn der Vergleich zeigt, dass der Audit-Hash-Wert nicht mit dem gültigen Hash-Wert übereinstimmt.

18. Das in Anspruch 17 beanspruchte Verfahren, wobei der Schritt des Anfertigens des Audit-Hash-Wertes durchgeführt wird in Verbindung mit einem geschützten Direktzugriffsspeicher (**407**).

19. Das in Anspruch 17 beanspruchte Verfahren, ferner enthaltend den Schritt:
Signieren des gültigen Hash-Wertes mit einer auf einem privaten Schlüssel basierenden digitalen Signatur.

20. Das in Anspruch 17 beanspruchte Verfahren, wobei der Schritt des Anfertigens des Audit-Hash-Wertes durchgeführt wird gemäß dem Ablauf eines Hardware-basierten Zeitgebers.

21. Das in Anspruch 17 beanspruchte Verfahren, wobei der Schritt des Anfertigens des Audit-Hash-Wertes das Berechnen von Audit-Hash-Wert-Segmenten involviert.

22. Das in Anspruch 21 beanspruchte Verfahren, wobei die Berechnung eines Audit-Hash-Wert-Segments, wenn nötig, verzögert werden kann, während andere Prozesse, die innerhalb der elektronischen Vorrichtung stattfinden, fertig gestellt werden.

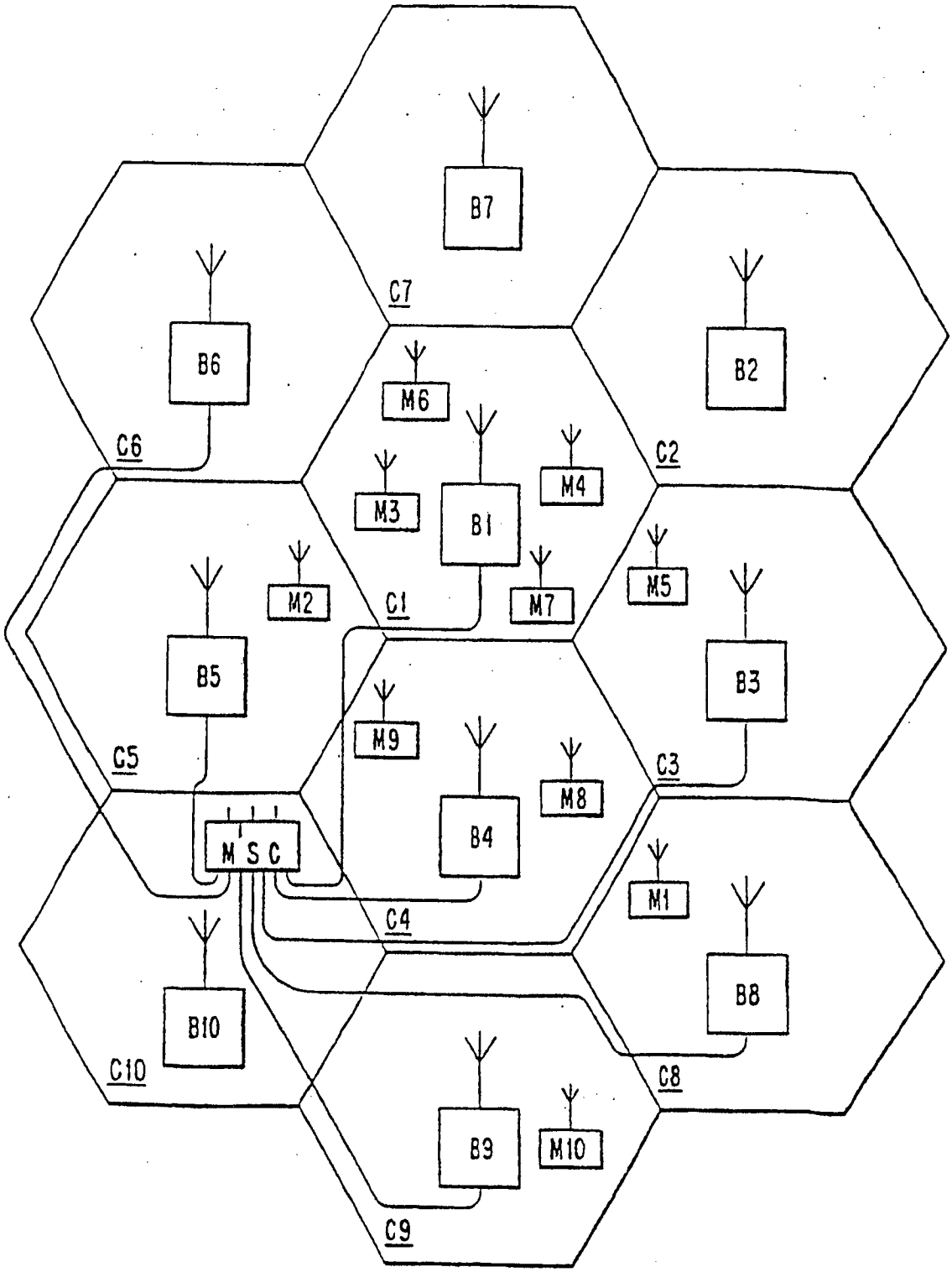
23. Das in Anspruch 17 beanspruchte Verfahren, wobei dem gültigen Hash-Wert eine digitale Signatur gegeben wird, und wobei der Schritt des Vergleichens des Audit-Hash-Wertes mit dem gültigen Hash-Wert den Schritt des Authentifizierens des gültigen Hash-Wertes gegen die Signatur enthält.

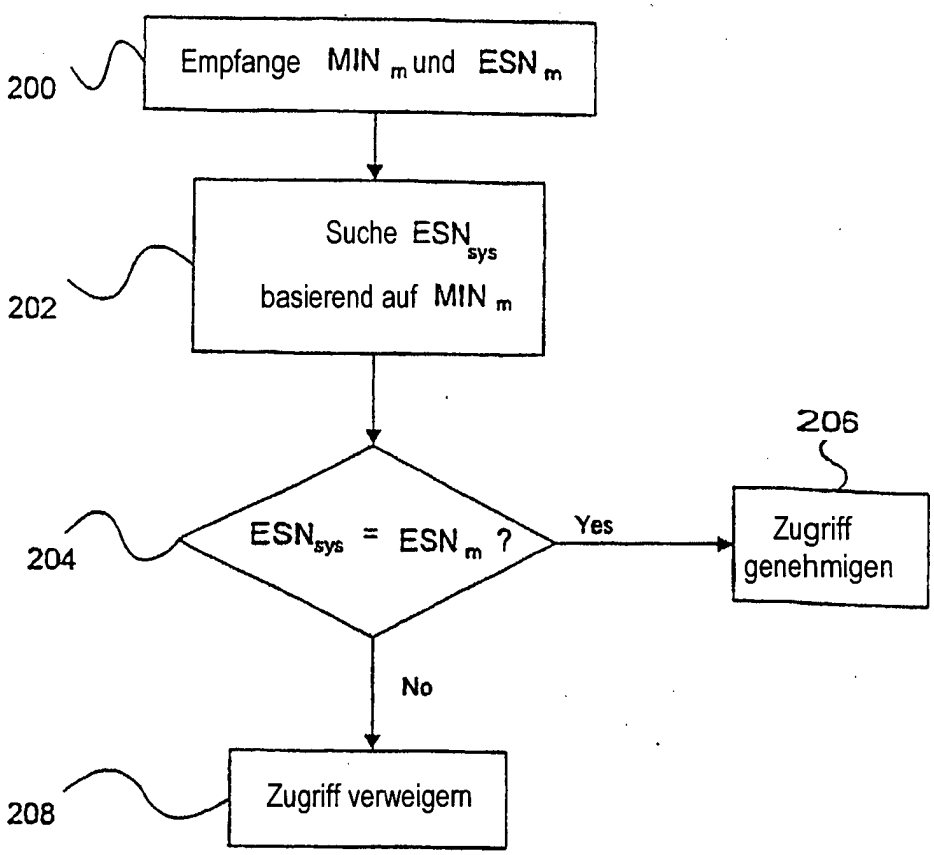
24. Das in Anspruch 17 beanspruchte Verfahren, wobei die elektronische Vorrichtung ein Mobiltelefon ist.

Es folgen 12 Blatt Zeichnungen

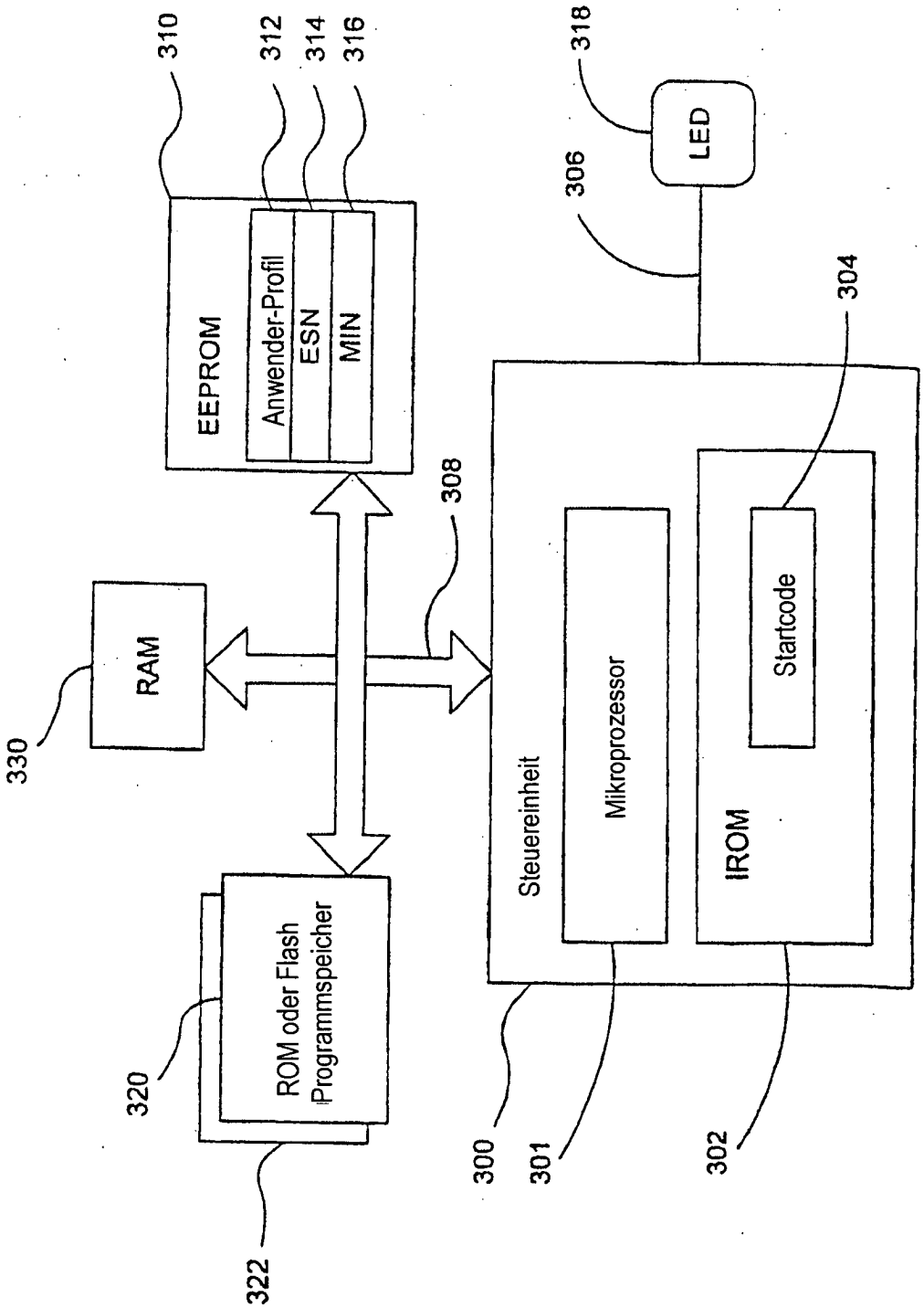
Anhängende Zeichnungen

Fig. 1

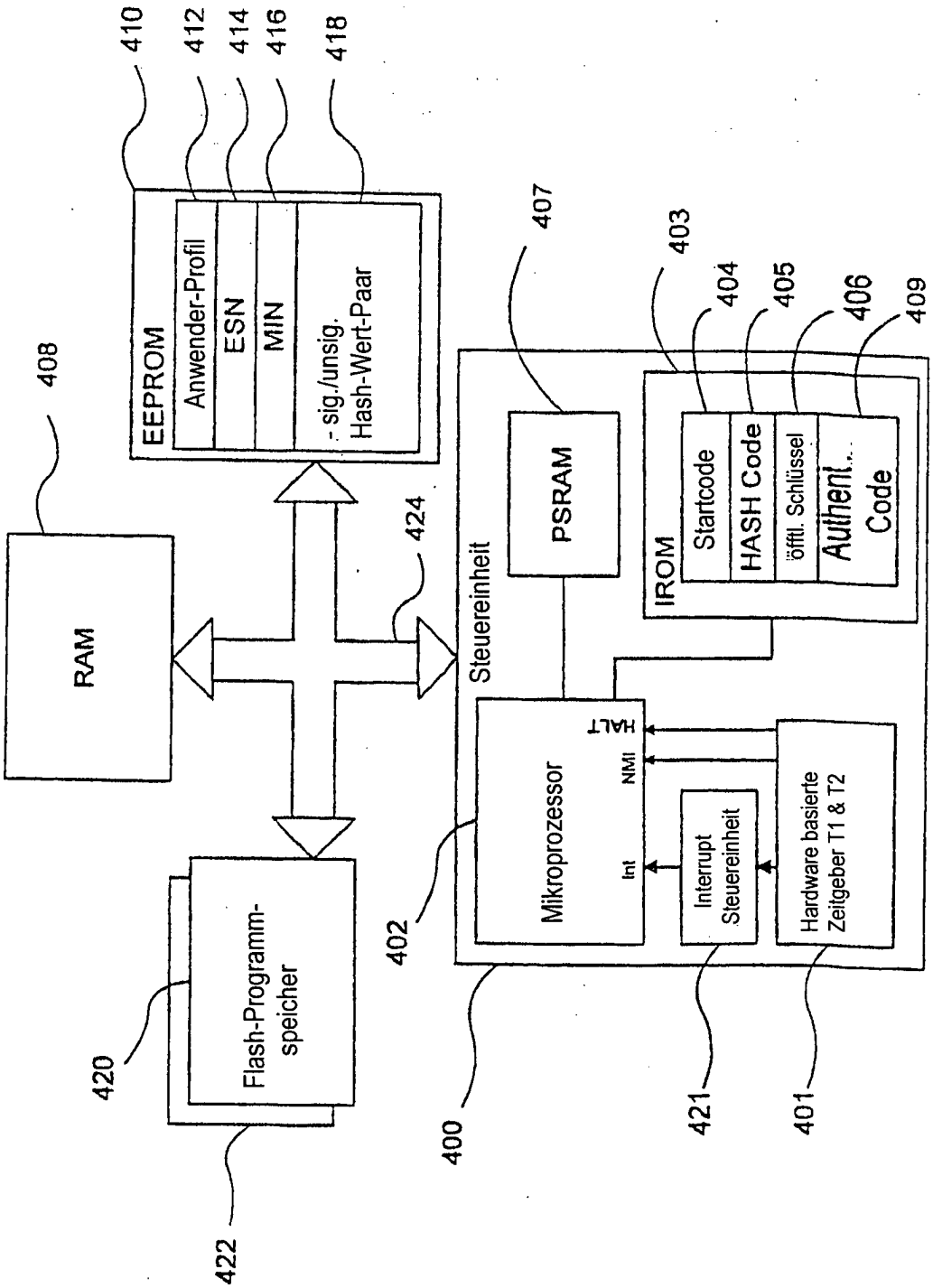



200
Empfange MIN m und ESN m
202
Suche ESN sys
basierend auf MIN m
204
ESN sys = ESN m ?
Yes
206
Zugriff genehmigen
No
208
Zugriff verweigern

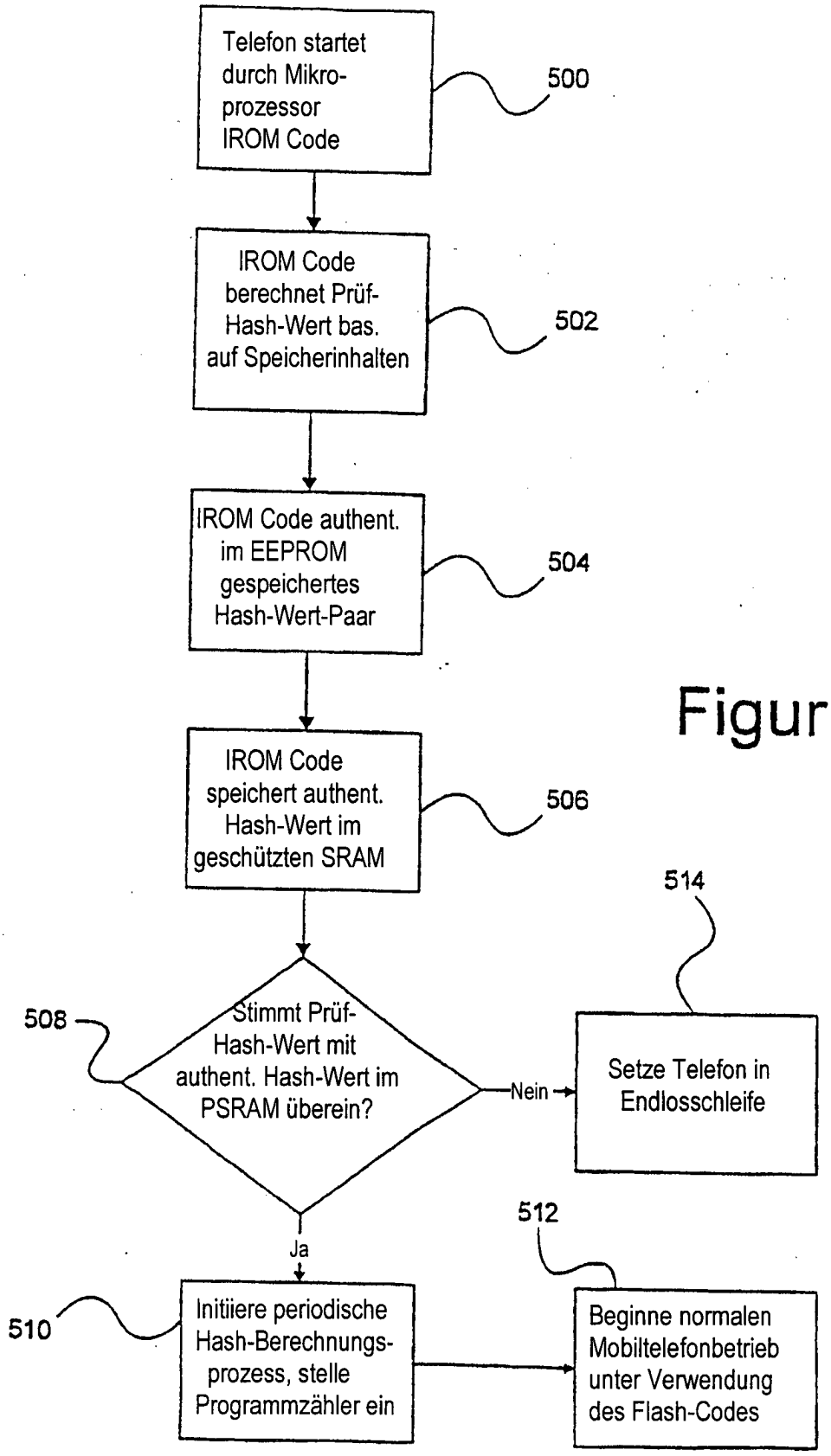
Figur 2


310
312
314
316
318
LED
306
EEPROM
Anwender-Profil
ESN
MIN
304
308
RAM
330
Steuereinheit
Mikroprozessor
IROM
Startcode
ROM oder Flash
Programmspeicher
320
322
300
301
302

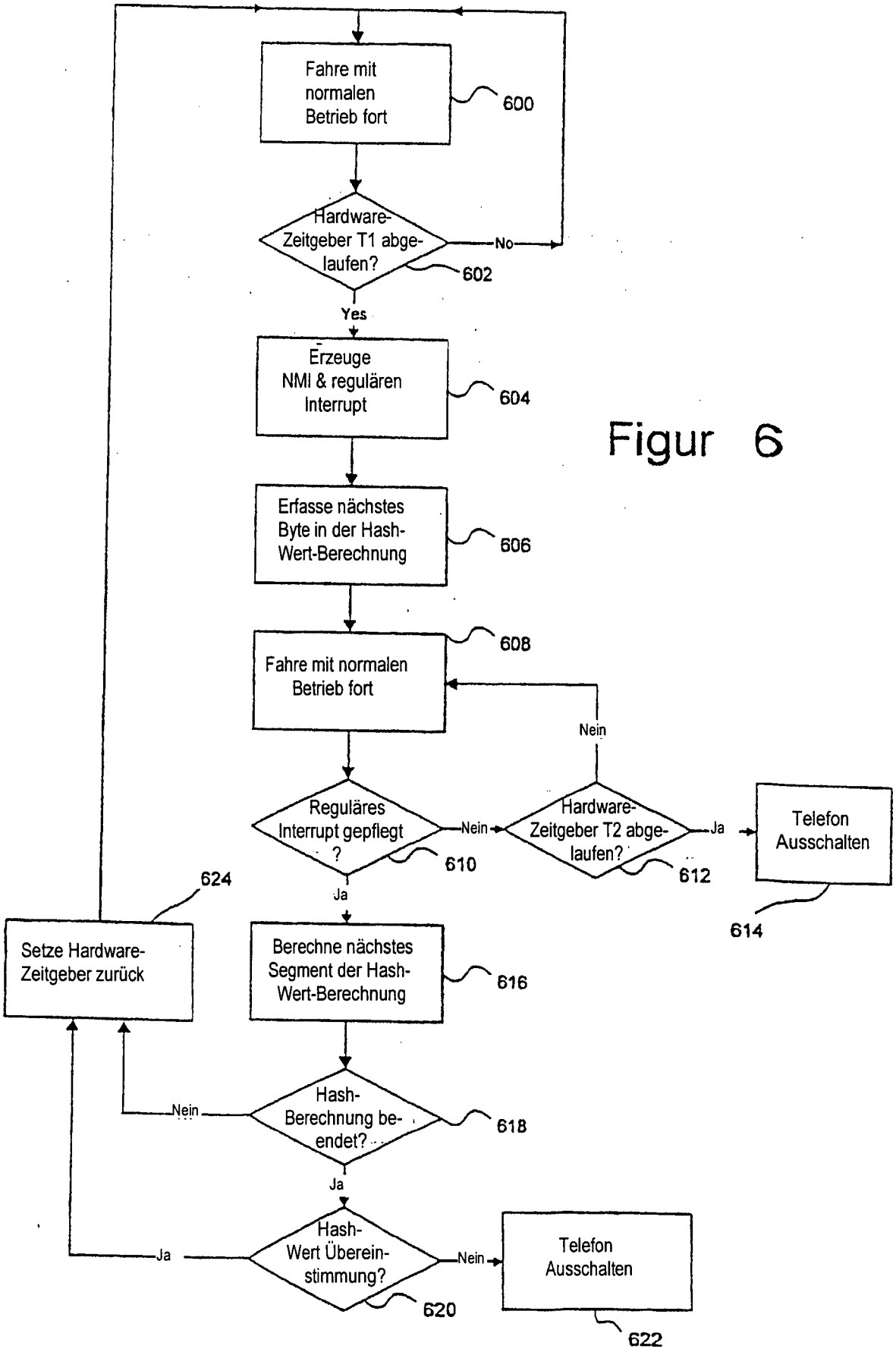
Figur 3


410
412
414
416
418
EEPROM
Anwender-Profil
ESN
MIN
- sig./unsig. Hash-Wert-Paar
408
RAM
424
407
403
404
405
406
409
PSRAM
IROM
Startcode
HASH Code
öfftl. Schlüssel
Authent... Code
Steuereinheit
HALT
NMI
Int
Mikroprozessor
Interrupt Steuereinheit
Hardware basierte Zeitgeber T1 & T2
402
400
421
401
420
Flash-Programm-speicher
422

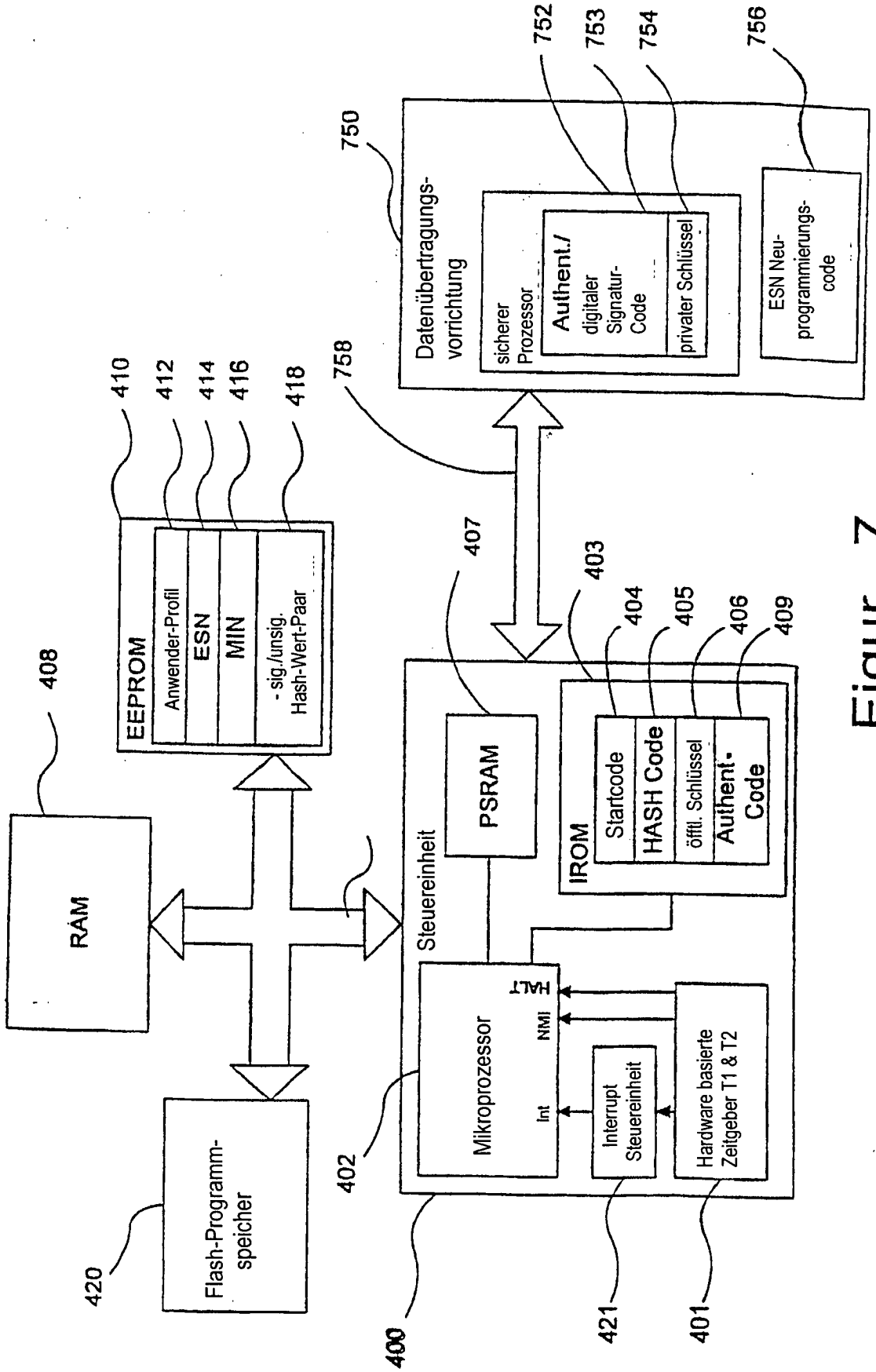
Figur 4


Telefon startet durch Mikro-prozessor IROM Code
500
IROM Code berechnet Prüf-Hash-Wert bas. auf Speicherinhalten
502
IROM Code authent. im EEPROM gespeichertes Hash-Wert-Paar
504
IROM Code speichert authent. Hash-Wert im geschützten SRAM
506
514
508
Stimmt Prüf-Hash-Wert mit authent. Hash-Wert im PSRAM überein?
Nein
Setze Telefon in Endlosschleife
Ja
512
510
Initiiere periodische Hash-Berechnungs-prozess, stelle Programmzähler ein
Beginne normalen Mobiltelefonbetrieb unter Verwendung des Flash-Codes

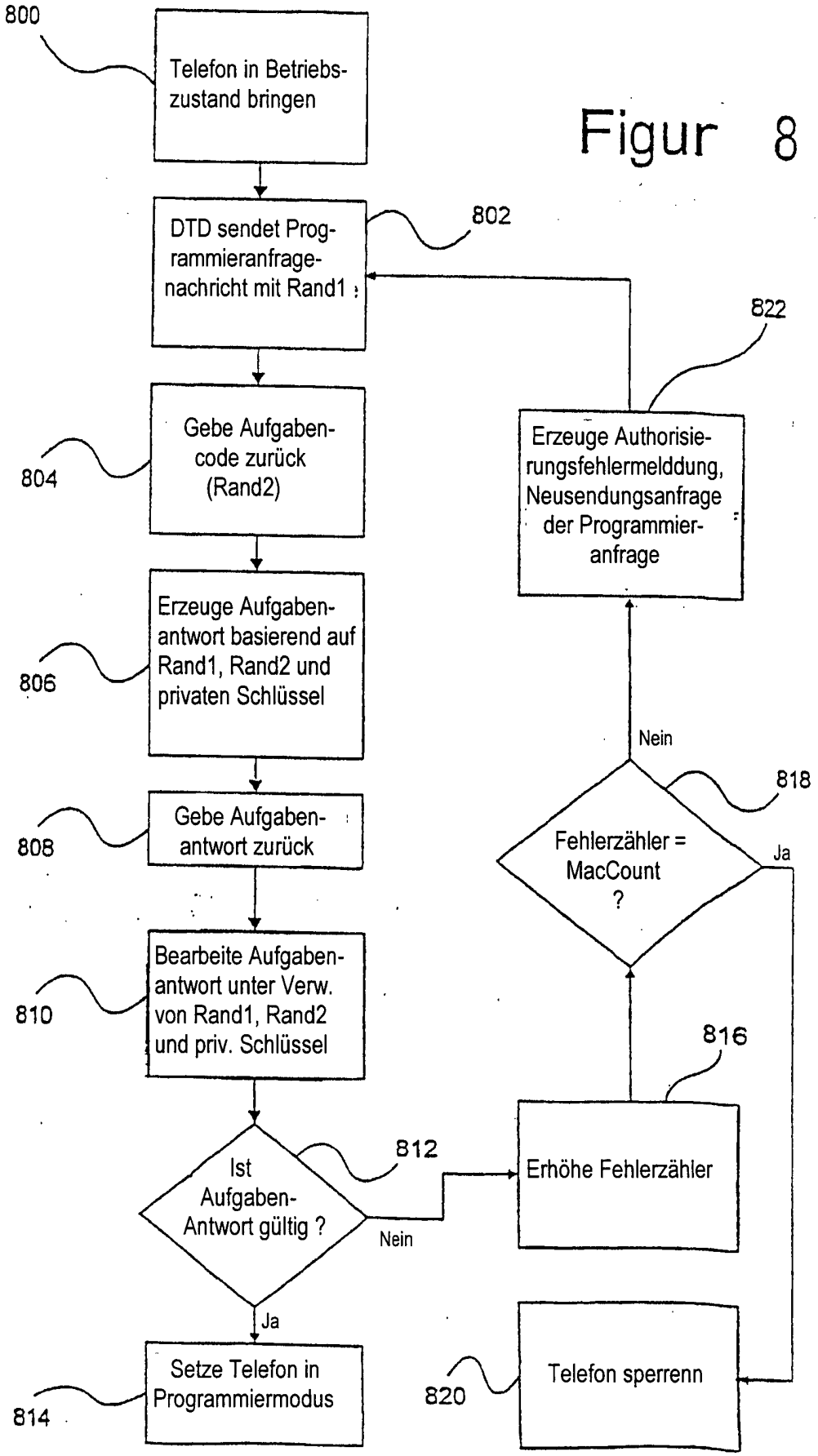
Figur 5


Fahre mit normalen Betrieb fort
600
Hardware-Zeitgeber T1 abgelaufen?
602
No
Yes
Erzeuge NMI & regulären Interrupt
604
Erfasse nächstes Byte in der Hash-Wert-Berechnung
606
Fahre mit normalen Betrieb fort
608
Nein
Reguläres Interrupt gepflegt ?
610
Nein
Hardware-Zeitgeber T2 abgelaufen?
612
Ja
Telefon Ausschalten
614
Ja
624
Setze Hardware-Zeitgeber zurück
Berechne nächstes Segment der Hash-Wert-Berechnung
616
Nein
Hash-Berechnung beendet?
618
Ja
Hash-Wert Übereinstimmung?
620
Ja
Nein
Telefon Ausschalten
622

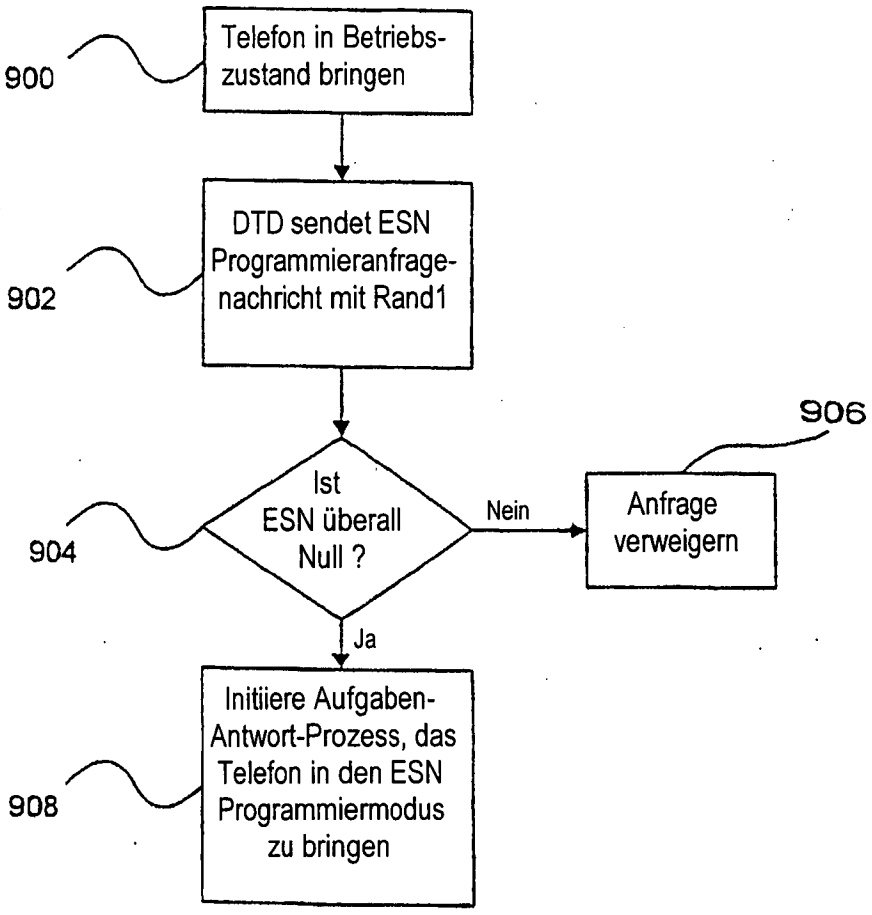
Figur 6


752
753
754
756
750
Datenübertragungs-vorrichtung
sicherer Prozessor
Authent./ digitaler Signatur-Code
privater Schlüssel
ESN Neu-programmierungs-code
758
410
412
414
416
418
EEPROM
Anwender-Profil
ESN
MIN
- sig./unsig. Hash-Wert-Paar
407
403
404
405
406
409
408
RAM
Steuereinheit
PSRAM
IROM
Startcode
HASH Code
öfftl. Schlüssel
Authent.-Code
HALT
NMI
Int
Mikroprozessor
Interrupt Steuereinheit
Hardware basierte Zeitgeber T1 & T2
402
420
Flash-Programm-speicher
400
421
401

Figur 7

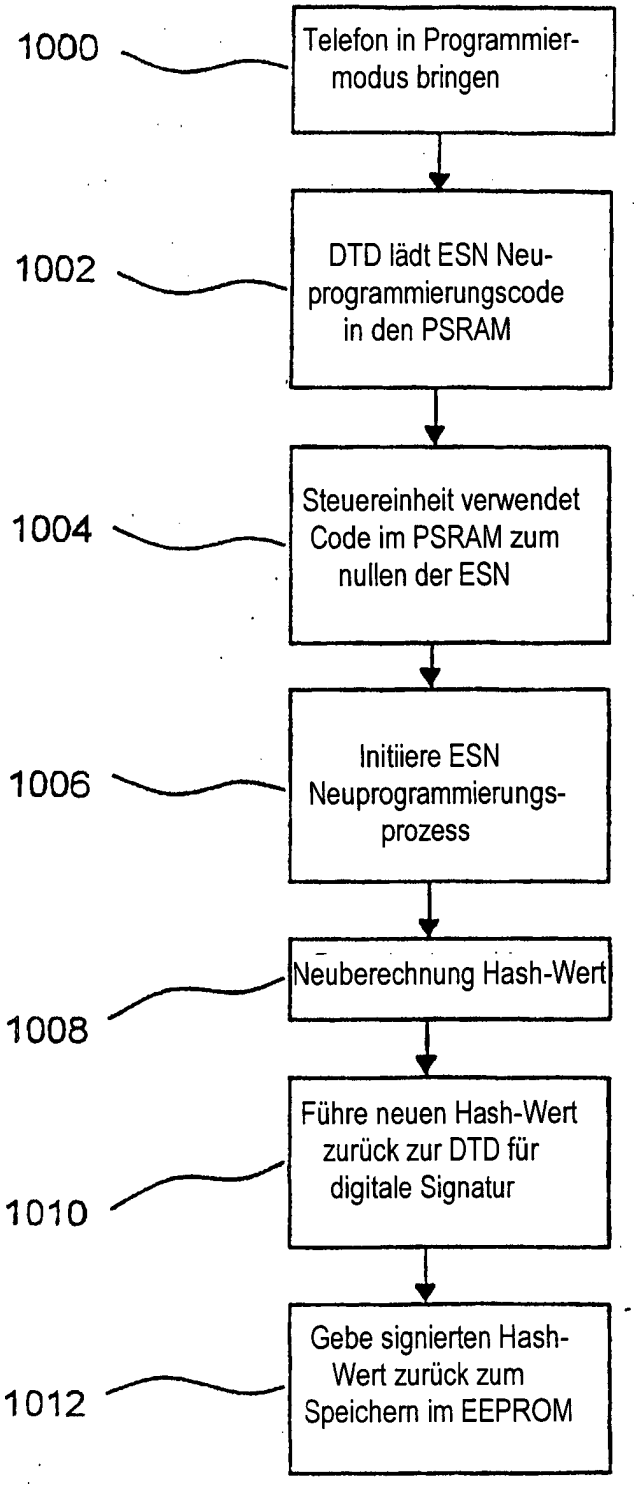

800
Telefon in Betriebs-zustand bringen
802
DTD sendet Prog-rammieranfrage-nachricht mit Rand1
804
Gebe Aufgaben-code zurück (Rand2)
806
Erzeuge Aufgaben-antwort basierend auf Rand1, Rand2 und privaten Schlüssel
808
Gebe Aufgaben-antwort zurück
810
Bearbeite Aufgaben-antwort unter Verw. von Rand1, Rand2 und priv. Schlüssel
812
Ist Aufgaben-Antwort gültig ?
Nein
Ja
814
Setze Telefon in Programmiermodus
816
Erhöhe Fehlerzähler
818
Fehlerzähler = MacCount ?
Nein
Ja
820
Telefon sperrenn
822
Erzeuge Authorisie-rungsfehlermelddung, Neusendungsanfrage der Programmier-anfrage

Figur 8


900
Telefon in Betriebs-zustand bringen
902
DTD sendet ESN Programmieranfrage-nachricht mit Rand1
904
Ist ESN überall Null ?
Nein
906
Anfrage verweigern
Ja
908
Initiiere Aufgaben-Antwort-Prozess, das Telefon in den ESN Programmiermodus zu bringen

Figur 9

FIG. 10


1000
Telefon in Programmier-modus bringen
1002
DTD lädt ESN Neu-programmierungscode in den PSRAM
1004
Steuereinheit verwendet Code im PSRAM zum nullen der ESN
1006
Initiiere ESN Neuprogrammierungs-prozess
1008
Neuberechnung Hash-Wert
1010
Führe neuen Hash-Wert zurück zur DTD für digitale Signatur
1012
Gebe signierten Hash-Wert zurück zum Speichern im EEPROM

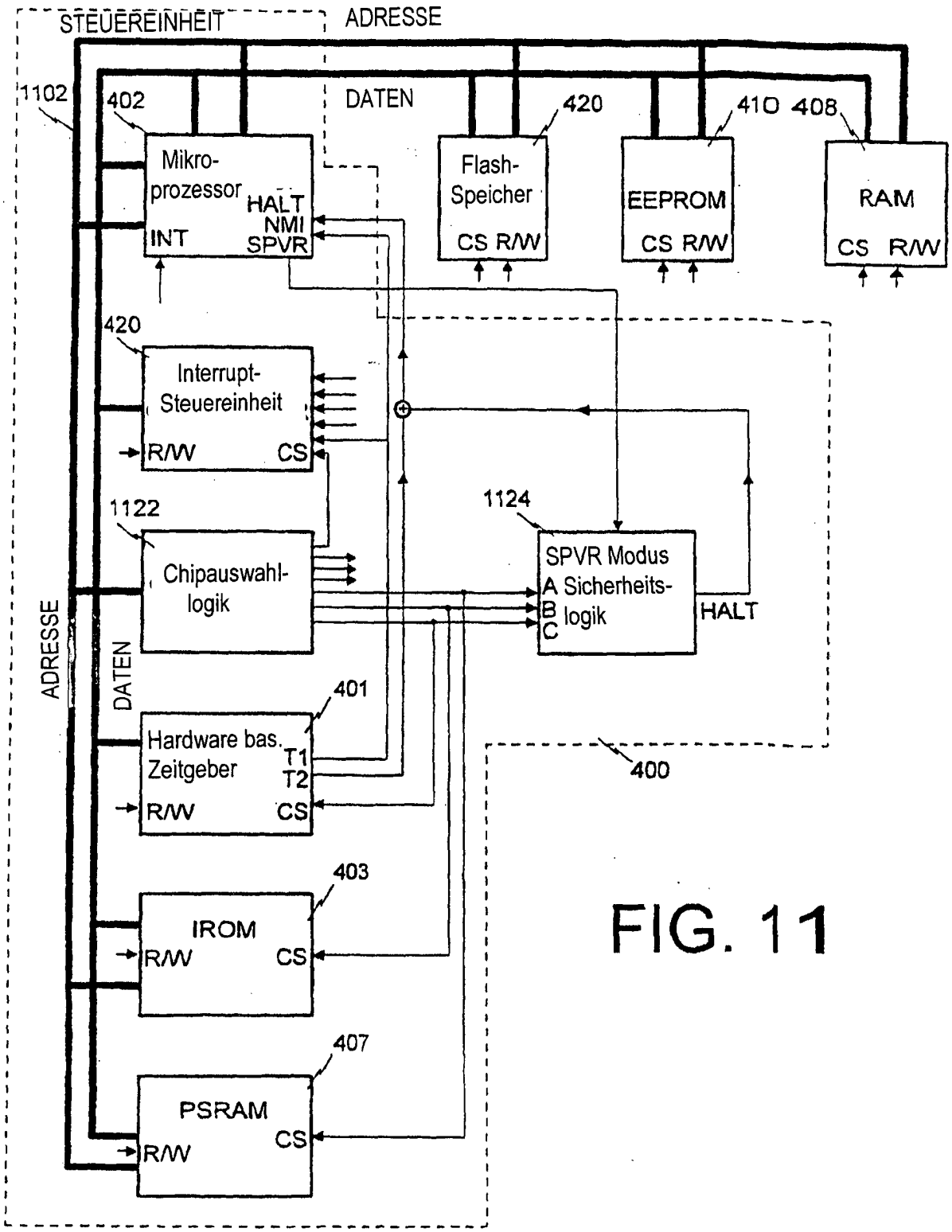
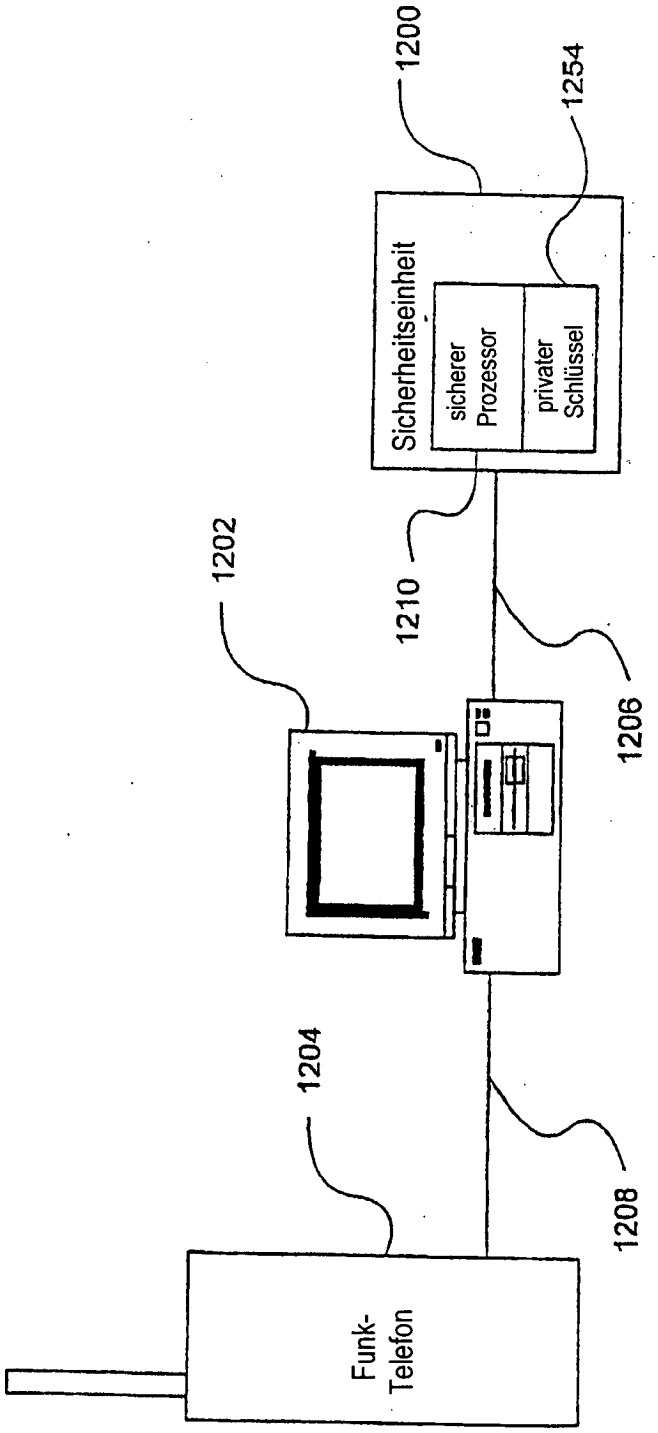

STEUEREINHEIT
ADRESSE
DATEN
1102
402
420
410
408
Mikro-
prozessor
HALT
NMI
SPVR
INT
Flash-
Speicher
CS R/W
EEPROM
CS R/W
RAM
CS R/W
420
Interrupt-
Steuereinheit
R/W
CS
1122
Chipauswahl-
logik
1124
SPVR Modus
A Sicherheits-
B logik
C
HALT
ADRESSE
DATEN
401
Hardware bas.
Zeitgeber
T1
T2
R/W
CS
400
403
IROM
R/W
CS
407
PSRAM
R/W
CS

FIG. 11


1200
1254
Sicherheitseinheit
sicherer Prozessor
privater Schlüssel
1210
1202
1206
1204
1208
Funk-Telefon

Figur 12