



(10) **DE 10 2016 005 419 A1** 2017.11.02

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2016 005 419.0**

(22) Anmeldetag: **02.05.2016**

(43) Offenlegungstag: **02.11.2017**

(51) Int Cl.: **H04W 12/00 (2009.01)**  
**G06F 9/445 (2006.01)**

(71) Anmelder:  
**Giesecke+Devrient Mobile Security GmbH, 81677  
München, DE**

(72) Erfinder:  
**Götze, Frank, 81379 München, DE; Dietze, Claus,  
82395 Obersöchering, DE; Eichholz, Jan, 80997  
München, DE**

(56) Ermittelter Stand der Technik:

<b>US</b>	<b>2013 / 0 295 997</b>	<b>A1</b>
<b>US</b>	<b>2014 / 0 194 103</b>	<b>A1</b>
<b>US</b>	<b>2014 / 0 220 952</b>	<b>A1</b>
<b>US</b>	<b>2015 / 0 134 958</b>	<b>A1</b>

Rechercheantrag gemäß § 43 PatG ist gestellt.

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.**

(54) Bezeichnung: **Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements**

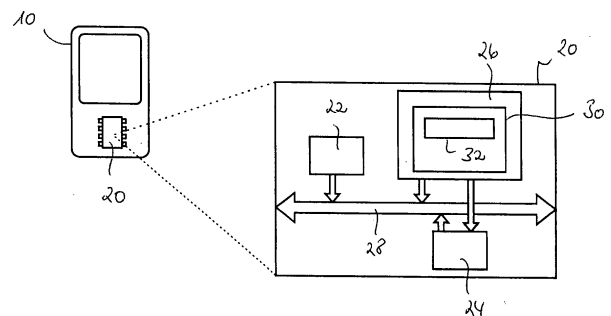
(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements (30), das der Nutzung von Diensten eines Mobilfunknetzwerks dient, in einem mobilen Endgerät (10). Bei dem Verfahren wird das sichere Element (30) gestartet und zu einer Übermittlung einer Statusnachricht aufgefordert. Das sichere Element (30) übermittelt eine Statusnachricht, in der angegeben ist, ob das sichere Element

S1) nur einen Bootloader (32), aber noch kein Firmware-Image für das sichere Element enthält,

S2) ein Firmware-Image für das sichere Element (30) enthält, aber noch nicht vollständig personalisiert, oder

S3) vollständig personalisiert ist.

Das sichere Element (30) wird in den Fällen S1), S2) und S3) akzeptiert, in anderen Fällen abgelehnt. Im Fall S1) wird für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements (30) initiiert.



## Beschreibung

**[0001]** Die Erfindung betrifft universelle integrierte Schaltungskarten (Universal Integrated Circuit Card, UICC) im Allgemeinen und betrifft vor allem Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements, insbesondere in Form einer UICC oder einer integrierten UICC (iUICC).

**[0002]** Heutige mobile Endgeräte sind meist eingerichtet um entfernbare universelle integrierte Schaltungskarten (UICC) aufzunehmen und zu betreiben. Eine vollständig personalisierte UICC ermöglicht dem mobilen Endgerät auf Dienste zuzugreifen, die von Betreibern mobiler Netzwerke (Mobile Network Operator, MNO) bereitgestellt werden. Die UICCs sind dabei derzeit als Karte oder als eingebettetes Modul (embedded UICC, eUICC) in verschiedenen Formfaktoren ausgeprägt. Insbesondere für eingebettete UICCs ist es dabei erforderlich, Daten und Teile des Betriebssystems über entsprechende Subskriptionsmanagementdienste pflegen zu können, also Daten und Programmteile anlegen, aktivieren, aktualisieren und löschen zu können.

**[0003]** Bei neuen Konzepten für mobile Endgeräte ist angedacht, die UICC nicht mehr als separates Element auszubilden, sondern in ein Ein-Chip-System des Endgeräts so zu integrieren, dass sie als in eine Sicherheitsumgebung des Ein-Chip-Systems geladene integrierte UICC (iUICC) vorliegt. In einem solchen Fall ist es wünschenswert, das gesamte Betriebssystem, nachfolgend auch als Firmware-Image bezeichnet, über einen Subskriptionsmanagementdienst in die Sicherheitsumgebung des mobilen Endgeräts laden und personalisieren zu können.

**[0004]** Derzeit ist zu diesem Zweck in der UICC ein Bootloader vorgesehen, der in der Regel vom Chiphersteller selbst bereitgestellt wird. Der Bootloader dient dazu, das von der UICC angefertigte Image, nämlich das oben genannte Firmware-Image, auf die UICC zu laden und dort zu installieren. Die Bootloader sind dabei so beschaffen, dass bestimmte Kommandosequenzen streng eingehalten und bestimmte Sicherheitsbedingungen erfüllt werden müssen. Wird versucht, heutige UICCs oder eUICCs, die nur einen Bootloader enthalten, in einem mobilen Endgerät in Betrieb zu nehmen, so führt dies zu einer Ablehnung der UICC durch den Baseband-Prozessor und der Ausgabe eine entsprechenden Fehlermeldung an den Benutzer. Eine nur mit einem Bootloader versehene UICC liefert beim Startup nämlich einen anderen Anwer-To-Reset (ATR) als eine vollständig personalisierte UICC. Weitere reguläre UICC Kommandos werden dann vom Bootloader ignoriert. Der Baseband-Prozessor schaltet als Folge die UICC ab, so dass diese nicht mehr für Subskriptionsmanage-

mentbefehle zugänglich ist und der Download eines Firmware-Images somit nicht mehr möglich ist.

**[0005]** Weiter werden mobile Endgeräte und insbesondere Smartphones häufig vom Betreiber eines mobilen Netzwerks subventioniert und beispielsweise über eine Vertragslaufzeit von ein bis zwei Jahren finanziert. Während dieser Vertragslaufzeit soll es für einen Kunden manchmal nur möglich sein, das Gerät mit einer bestimmten SIM-Karte, in einem bestimmten Mobilfunknetz oder mit anderen Einschränkungen zu nutzen. Die derzeit zu diesem Zweck eingesetzten Verfahren sind allerdings nicht für integrierte UICCs geeignet. Es ist dabei davon auszugehen, dass mobile Endgeräte in diesem Fall mit einem generischen Bootloader ausgeliefert werden, der das Laden von iUICCs verschiedener Netzbetreiber ermöglicht.

**[0006]** Ausgehend davon liegt Erfindung die Aufgabe zugrunde, die Nachteile des Stands der Technik zu vermeiden. Insbesondere soll ein Verfahren angegeben werden, dass eine erfolgreiche erstmalige Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements erlaubt.

**[0007]** Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Weiterbildungen der Erfindung sind Gegenstand der abhängigen Ansprüche.

**[0008]** Die Erfindung stellt ein Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements in einem mobilen Endgerät bereit, wobei das sichere Element der Nutzung von Diensten eines Mobilfunknetzwerks dient. Bei dem Verfahren

- wird das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht aufgefordert,
- übermittelt das sichere Element eine Statusnachricht, in der angegeben ist, ob das sichere Element
  - S1) nur einen Bootloader, aber noch kein Firmware-Image für das sichere Element enthält,
  - S2) ein Firmware-Image für das sichere Element enthält, aber noch nicht vollständig personalisiert, oder
  - S3) vollständig personalisiert ist,
- wird das sichere Element in den Fällen S1), S2) und S3) akzeptiert, in anderen Fällen abgelehnt, und
- wird im Fall S1) für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert.

**[0009]** Das sichere Element ist vorteilhaft als universelle integrierte Schaltungskarte (UICC) ausgebildet, oder ist als integrierte UICC (iUICC) ausgebildet, die in eine Sicherheitsumgebung des mobilen Endgeräts geladen ist. Vorteilhaft enthält das mobile Endgerät

hierzu ein Ein-Chip-System mit einer Sicherheitsumgebung, beispielsweise in Form eines sicheren Prozessors, in die die iUICC geladen ist.

**[0010]** Bei einer vorteilhaften Verfahrensführung wird im Fall S2) eine Subskription bei einem Mobilfunknetzanbieter und/oder im Fall S3) eine SIM-Initialisierung durchgeführt.

**[0011]** Die Erfindung enthält auch ein Verfahren zur erstmaligen Inbetriebnahme eines noch kein Firmware-Image enthaltenen sicheren Elements in einem mobilen Endgerät, wobei das sichere Element der Nutzung von Diensten eines Mobilfunknetzwerks dient. Bei dem Verfahren

- wird das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht und zur Abarbeitung von Befehlen aufgefordert,
- übermittelt das sichere Element auf die Aufforderung hin eine erwartete Statusnachricht und quittiert die Abarbeitung der Befehle positiv um sicherzustellen, dass das sichere Element bei der erstmaligen Inbetriebnahme akzeptiert wird, und
- wird für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert.

**[0012]** Diese Vorgehensweise ist insbesondere dann gut geeignet, wenn das weiter oben beschriebene Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements nicht zum Erfolg führt, beispielsweise weil der Baseband-Prozessor des mobilen Endgeräts nicht zum Empfang der beschriebenen Statusnachrichten eingerichtet ist.

**[0013]** Es ist auch natürlich auch möglich und oft sogar besonders vorteilhaft, die beiden genannten Vorgehensweisen miteinander zu kombinieren. Dies gilt insbesondere dann, wenn vorab nicht bekannt ist, ob der Baseband-Prozessor des mobilen Endgeräts zum Empfang der beschriebenen Statusnachrichten eingerichtet ist oder nicht. Es kann dabei insbesondere zunächst eine Statusnachricht der genannten Art übermittelt werden und im Misserfolgsfall auf die zweitgenannte Vorgehensweise zurückzugreifen.

**[0014]** Bei der konkreten Umsetzung kommen verschiedene Kombinationsmöglichkeiten in Betracht, beispielsweise kann das sichere Element nach einer nicht akzeptierten Statusnachricht in kurzem zeitlichen Abstand erneut zur Übermittlung einer Statusnachricht aufgefordert werden und aus dem kurzen zeitlichen Abstand der beiden Aufforderungen darauf schließen, dass der Baseband-Prozessor des mobilen Endgeräts nicht zum Empfang solcher Statusnachrichten eingerichtet ist, und die erneute Aufforderung dann auf die alternativ genannte Art durch Simulation der Antwort eines bereits vollständig personalisierten sicheren Elements beantworten.

**[0015]** Bei einem kombinierten Verfahren zur erstmaligen Inbetriebnahme eines noch kein Firmware-Image enthaltenen sicheren Elements in einem mobilen Endgerät, wobei das sichere Element der Nutzung von Diensten eines Mobilfunknetzwerks dient, ist dann vorgesehen, dass

- das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht aufgefordert wird,
- das sichere Element auf eine erste Aufforderung hin eine Statusnachricht übermittelt, in der angegeben ist, dass das sichere Element S1) nur einen Bootloader, aber noch kein Firmware-Image für das sichere Element enthält, und
- falls die Statusnachricht nicht akzeptiert wird, das sichere Element auf eine weitere Aufforderung hin eine erwartete Statusnachricht übermittelt und auf eine Aufforderung zur Abarbeitung von Befehlen die Abarbeitung der Befehle positiv quittiert um sicherzustellen, dass das sichere Element bei der erstmaligen Inbetriebnahme akzeptiert wird, und
- für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert wird.

**[0016]** Auch hierbei ist das sichere Element ist vorteilhaft als universelle integrierte Schaltungskarte (UICC) ausgebildet, oder ist als integrierte UICC (iUICC) ausgebildet, die in eine Sicherheitsumgebung des mobilen Endgeräts geladen ist. Vorteilhaft enthält das mobile Endgerät hierzu ein Ein-Chip-System mit einer Sicherheitsumgebung, beispielsweise in Form eines sicheren Prozessors, in die die iUICC geladen ist.

**[0017]** Ein weiteres Ziel besteht vorliegend darin, auch bei einer in eine Sicherheitsumgebung eines mobile Endgeräts geladenen integrierte UICC (iUICC) eine Netzbindung des mobilen Endgeräts für einen bestimmten Zeitraum zu ermöglichen.

**[0018]** Um dieses weitere Ziel zu erreichen wird, um die Netzbindung einer in eine Sicherheitsumgebung eines mobilen Endgeräts geladenen iUICC sicherzustellen, eine Start-UICC in die Sicherheitsumgebung geladen, die keine Subskriptionsdaten enthält, die aber Regeln zur Auswahl von ein spielbaren Subskriptionsdaten enthält, und die nicht unautorisiert aus der Sicherheitsumgebung entfernbar ist.

**[0019]** Die Start-UICC kann insbesondere über einen generischen Bootloader in die Sicherheitsumgebung geladen werden, mit dem das mobile Endgerät anfänglich, beispielsweise vom OEM des Smartphones ausgestattet ist.

**[0020]** Eine Autorisierung zur Entfernung der Start-UICC kann beispielsweise über die Eingabe eines Codes erfolgen. Auch die Regeln zur Auswahl der

einspielbaren Subskriptionsdaten können mit Vorteil nur autorisiert geändert werden. Dies kann beispielsweise nach Ablauf der gewünschten Netzbindungsdauer durch einen Server erfolgen.

**[0021]** Weiter ist der generische Bootloader vorteilhaft derart gesperrt, dass die Start-IUICC nicht entfernt und keine zusätzliche IUICC in die Sicherheitsumgebung geladen werden kann. Auch der generische Bootloader kann mit Vorteil nur autorisiert gesperrt werden.

**[0022]** Bei einem späteren Aufbringen von Subskriptionsdaten in die Start-IUICC prüft diese, ob die Subskriptionsdaten konform zu den genannten Auswahlregeln sind. Ist dies der Fall, wird die Subskription durchgeführt, anderenfalls von der Start-IUICC abgelehnt.

**[0023]** Alternativ kann die Start-IUICC auch so ausgebildet sein, dass sie ein vollständiges Profil einschließlich Subskriptionsdaten enthält. Der generische Bootloader ist in diesem Fall so ausgebildet, dass er nur autorisierte iUICCs lädt, dass nur genau eine iUICC geladen sein kann, und dass eine Entfernung einer geladenen iUICC nur durch eine autorisierte Aktion erfolgen kann. In der Sicherheitsumgebung sind darüber hinaus mit Vorteil Routinen zur Verifikation einer geladenen iUICCs inklusive der Subskriptionsdaten hinterlegt, die bei jedem Laden einer iUICC in den Speicher der Sicherheitsumgebung abgearbeitet werden.

**[0024]** Weitere Ausführungsbeispiele sowie Vorteile der Erfindung werden nachfolgend anhand der Figur erläutert, bei deren Darstellung auf eine maßstabs- und proportionsgetreue Wiedergabe verzichtet wurde, um die Anschaulichkeit zu erhöhen.

**[0025]** Es zeigt:

**[0026]** Fig. 1 schematisch ein mobiles Endgerät mit einem Ein-Chip-System zur Erläuterung der Vorgehensweise bei einem erfindungsgemäßen Verfahren.

**[0027]** Die Erfindung wird nun am Beispiel der erstmaligen Inbetriebnahme einer iUICC (integrated IUICC) in einem mobilen Endgerät erläutert. Fig. 1 zeigt dazu schematisch ein mobiles Endgerät **10** mit einem Ein-Chip-System **20**, das einen Applikationsprozessor **22**, einen Baseband-Prozessor **24** und eine Sicherheitsumgebung **26** aufweist. Die verschiedenen Komponenten des Ein-Chip-Systems **20** kommunizieren miteinander über einen Systembus **28**.

**[0028]** Im Speicher der Sicherheitsumgebung **26** ist eine IUICC **30** abgelegt, die nur einen Bootloader **32**, aber noch kein Firmware-Image für die IUICC **30** enthält. Bei der erstmaligen Inbetriebnahme der IUICC bootet beim Starten des Ein-Chip-Systems **20** zu-

nächst der Applikationsprozessor **22** und startet den Baseband-Prozessor **24**. Dann wird, initiiert entweder durch den Baseband-Prozessor **24** oder den Applikationsprozessor **22**, die IUICC **30** in der Sicherheitsumgebung **26** gestartet und zur Übermittlung einer Statusnachricht aufgefordert.

**[0029]** Als Antwort übermittelt der Bootloader **32** der IUICC **30** eine Statusnachricht an den Baseband-Prozessor **24**, in der angegeben ist, ob die IUICC **30** nur einen Bootloader **32**, aber noch kein Firmware-Image für die IUICC **30** enthält (Fall S1), ob die IUICC **30** bereits ein Firmware-Image enthält aber noch nicht vollständig personalisiert ist (Fall S2), oder ob die IUICC **30** bereits vollständig personalisiert ist (Fall S3).

**[0030]** Der Baseband-Prozessor **24** ist dabei so eingerichtet, dass er die IUICC **30** in der der Sicherheitsumgebung **26** in den Fällen S1), S2), und S3) akzeptiert, in anderen Fällen ablehnt. Je nach dem empfangenen Status kann der Baseband-Prozessor **24** weitere Aktionen initiieren. Beispielsweise wird im Fall S1) für die erstmalige Inbetriebnahme ein Download des Firmware-Image der IUICC **30** durchgeführt. Im Fall S2), in dem das Firmware-Image bereits vorliegt, kann mit Hilfe des Applikationsprozessors **22** eine Subskription durchgeführt werden, und im Fall S3) kann eine SIM-Initialisierung erfolgen.

**[0031]** Selbst wenn der Baseband-Prozessor **24** nicht wie oben beschrieben eingerichtet ist, kann der Bootloader **32** dennoch erreichen, dass die IUICC **30** vom Baseband-Prozessor **24** bei der erstmaligen Inbetriebnahme nicht abgelehnt wird. Dazu ist der Bootloader **32** der IUICC **30** so konfiguriert, dass er die vom Baseband-Prozessor **24** empfangenen Kommandos abarbeitet, ohne jedoch die jeweils dahinterstehende Funktionalität vollständig zur Verfügung zu stellen. Beispielsweise werden in der Start-up-Sequenz vom Baseband-Prozessor **24** verschiedene Dateien selektiert und ausgelesen. Anstatt nun das Dateisystem selbst zu Verfügung zu stellen, ist der Bootloader **32** so eingerichtet, dass er die Existenz dieser Dateien lediglich simuliert, indem entsprechende Anfragen positiv quittiert werden.

**[0032]** Beispielsweise liefert der Bootloader **32** beim Auslesen einer Datei den minimalen leeren Defaultwert zurück, der pro Datei erwartet wird. Dies kann für eine Datei NULL sein, oder eine minimale Anzahl an Bytes mit leerem Eintrag, je nach Kontext etwa FF oder 00, oder ein Defaultwert nach Annex E der Spezifikation TS 31.102. Eine Authentisierungsanfrage wird mit einer entsprechenden Fehlermeldung quittiert. Befehle zum Beschreiben der Dateien werden gegenüber dem Baseband-Prozessor **24** zwar positiv quittiert, allerdings wird beim erneuten Lesen wieder der oben beschriebene Defaultwert geliefert. Insgesamt antwortet der Bootloader **32** auf die Anfragen

des Baseband-Prozessors **24** wie von diesem erwartet und wird daher nicht als ungültige SIM abgelehnt, so dass nach dem Starten der iUICC **30** der gewünschte Download des Firmware-Images durchgeführt werden kann.

**[0033]** Die zuletzt beschriebene Vorgehensweise kann auch erst dann durchgeführt werden, wenn die Übermittlung der zuerst beschriebenen Statusnachricht an den Baseband-Prozessor **24** gescheitert ist. Dabei übermittelt der Bootloader **32** auf die Anfrage des Baseband-Prozessors **24** zunächst die oben genannte Statusnachricht S1) mit dem Inhalt, dass die iUICC **30** nur einen Bootloader **32**, aber noch kein Firmware-Image für das sichere Element enthält. Ist der Baseband-Prozessor **24** für den Empfang solcher Statusnachrichten eingerichtet, wird die Statusnachricht und damit die iUICC **30** akzeptiert und anschließend ein Download für ein Firmware-Image durchgeführt, wie oben beschrieben.

**[0034]** Wird die Statusnachricht S1) nicht akzeptiert, so schließt der Bootloader **32** darauf, dass der Baseband-Prozessor **24** des mobilen Endgeräts **10** nicht für den Empfang solcher Statusnachrichten eingerichtet ist und wählt als alternative Vorgehensweise bei einer erneuten Anfrage des Baseband-Prozessors **24** die oben beschriebene Simulation des ATR einer bereits vollständig personalisierten UICC. Nach dem erfolgreichen Passieren der Startup-Sequenz kann auch in diesem Fall der gewünschte Download des Firmware-Images durchgeführt werden.

**[0035]** In beiden beschriebenen Fällen bleibt die nur mit einem Bootloader **32** ausgestattete iUICC betriebsbereit und steht daher für Subskriptionsmanagementdienste zur Verfügung. Ein Abschalten des sicheren Elements durch den Baseband-Prozessor **24** wird verhindert. Im erstgenannten Fall kennt der Baseband-Prozessor **24** sogar den Status der iUICC **30** und kann daher statusabhängig entsprechende weitere Aktionen starten.

**[0036]** Die beschriebene Vorgehensweise kann auch bei klassischen UICCs im SIM-Karten-Formfaktor, sowie bei eingebetteten UICCs (eUICC) angewandt werden, sofern diese Plattformen einen Software-Image-Download unterstützen.

**[0037]** Falls die Hardware-Plattform zur Abbildung multipler SIM-Lösungen mehrere UICC-Plattformen parallel unterstützt, so werden alle Anfragen gemäß der oben beschriebenen Vorgehensweise beantwortet.

**[0038]** In einer Weiterbildung ist auch möglich, dass der oben beschriebene Bootloader **32** eine initiale minimale Subskription enthält, die zu einem Einbuchen in ein Mobilfunknetzwerk genutzt werden kann, mit der aber nur ein Software-Image und die zugehö-

rigen Personalisierungsdaten geladen werden können.

## Patentansprüche

1. Verfahren zur erstmaligen Inbetriebnahme eines nicht vollständig personalisierten sicheren Elements, das der Nutzung von Diensten eines Mobilfunknetzwerks dient, in einem mobilen Endgerät, wobei bei dem Verfahren

- das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht aufgefordert wird,
- das sichere Element eine Statusnachricht übermittelt, in der angegeben ist ob das sichere Element S1) nur einen Bootloader, aber noch kein Firmware-Image für das sichere Element enthält, S2) ein Firmware-Image für das sichere Element enthält, aber noch nicht vollständig personalisiert, oder S3) vollständig personalisiert ist,
- das sichere Element in den Fällen S1), S2) und S3) akzeptiert, in anderen Fällen abgelehnt wird, und
- im Fall S1) für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass das sichere Element als universelle integrierte Schaltungskarte (Universal Integrated Circuit Card, UICC) ausgebildet ist.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass das sichere Element als integrierte UICC (iUICC) ausgebildet ist, die in eine Sicherheitsumgebung des mobilen Endgeräts geladen ist.

4. Verfahren nach wenigstens einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass im Fall S2) eine Subskription bei einem Mobilfunknetzanbieter und/oder im Fall S3) eine SIM-Initialisierung durchgeführt wird.

5. Verfahren zur erstmaligen Inbetriebnahme eines noch kein Firmware-Image enthaltenden sicheren Elements, das der Nutzung von Diensten eines Mobilfunknetzwerks dient, in einem mobilen Endgerät, wobei bei dem Verfahren

- das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht und zur Abarbeitung von Befehlen aufgefordert wird,
- das sichere Element auf die Aufforderung hin eine erwartete Statusnachricht übermittelt und die Abarbeitung der Befehle positiv quittiert um sicherzustellen, dass das sichere Element bei der erstmaligen Inbetriebnahme akzeptiert wird, und
- für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert wird.

6. Verfahren zur erstmaligen Inbetriebnahme eines noch kein Firmware-Image enthaltenden sicheren Ele-

ments, das der Nutzung von Diensten eines Mobilfunknetzwerks dient, in einem mobilen Endgerät, wobei bei dem Verfahren

- das sichere Element gestartet und zu einer Übermittlung einer Statusnachricht aufgefordert wird,
- das sichere Element auf eine erste Aufforderung hin eine Statusnachricht übermittelt, in der angegeben ist, dass das sichere Element S1) nur einen Bootloader, aber noch kein Firmware-Image für das sichere Element enthält, und
- falls die Statusnachricht nicht akzeptiert wird, das sichere Element auf eine weitere Aufforderung hin eine erwartete Statusnachricht übermittelt und auf eine Aufforderung zur Abarbeitung von Befehlen die Abarbeitung der Befehle positiv quittiert um sicherzustellen, dass das sichere Element bei der erstmaligen Inbetriebnahme akzeptiert wird, und
- für die erstmalige Inbetriebnahme ein Download für ein Firmware-Image des sicheren Elements initiiert wird.

7. Verfahren nach Anspruch 5 oder 6, **dadurch gekennzeichnet**, dass das sichere Element als universelle integrierte Schaltungskarte (Universal Integrated Circuit Card, UICC) ausgebildet ist.

8. Verfahren nach Anspruch 5 oder 6, **dadurch gekennzeichnet**, dass das sichere Element als integrierte UICC (iUICC) ausgebildet ist, die in eine Sicherheitsumgebung des mobilen Endgeräts geladen ist.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

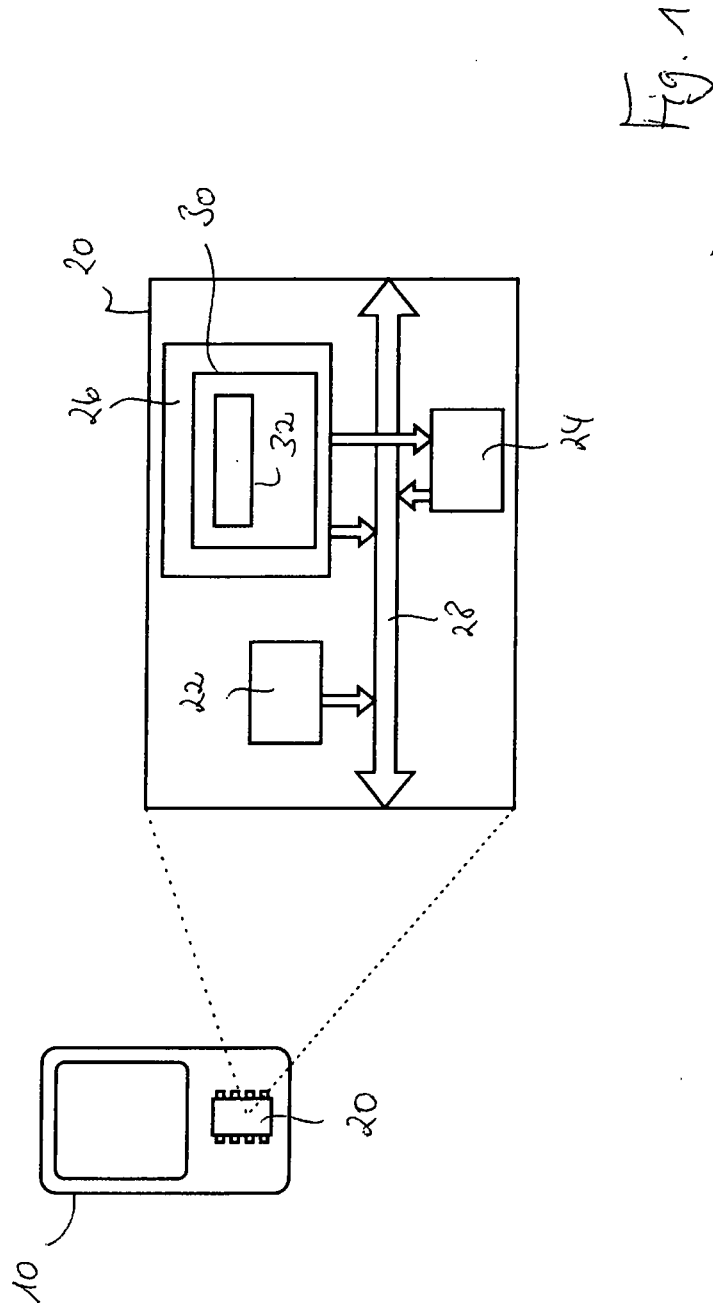


Fig. 1