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

(10) **DE 600 37 342 T2** 2008.11.27

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 301 909 B1**
(21) Deutsches Aktenzeichen: **600 37 342.8**
(86) PCT-Aktenzeichen: **PCT/NL00/00510**
(96) Europäisches Aktenzeichen: **00 948 414.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 2002/009046**
(86) PCT-Anmeldetag: **20.07.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **31.01.2002**
(97) Erstveröffentlichung durch das EPA: **16.04.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.12.2007**
(47) Veröffentlichungstag im Patentblatt: **27.11.2008**

(51) Int Cl.[8]: ***G07F 7/10*** (2006.01)

(73) Patentinhaber:
Belle Gate Investment B.V., Den Haag, NL

(74) Vertreter:
Patentanwälte Isenbruck Bösl Hörschler Wichmann Huhn, 68165 Mannheim

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(72) Erfinder:
DE JONG, Eduard Karel, NL-1012 DV Amsterdam, NL

(54) Bezeichnung: **VERFAHREN UND SYSTEM FÜR KOMMUNIZIERENDE GERÄTE, UND VORRICHTUNGEN DAFÜR, MIT GESCHÜTZTER DATENÜBERTRAGUNG**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf ein Verfahren zur Kommunikation zwischen einem ersten Gerät und einem zweiten Gerät. Die Erfindung ist insbesondere anwendbar auf dem Gebiet der Smart Cards, welche mit Endgeräten kommunizieren.

Stand der Technik

[0002] Kommunikationen zwischen Smart Cards und Endgeräten (Terminals) werden üblicherweise eingesetzt, um eines aus einer Mehrzahl sicherer Protokolle durchzuführen, welche erforderlich sind für einen durch die Smart Cards bereitzustellenden Service.

[0003] Insbesondere wenn eine kontaktlose Smart Card verwendet wird, kann sich ein Problem aus dem fluktuierenden Versorgungsstrom vom Endgerät zu der Smart Card aufgrund der Bewegung der Smart Card durch ein Energie bereitstellendes elektromagnetisches Feld ergeben. Diese Energiefluktuationen können derart stark und schnell sein, dass die Smart Card die Energieversorgung verlieren kann, bevor alle Kommunikationsschritte, die von einem Protokoll gefordert werden, durchgeführt worden sind. Was erforderlich ist, ist ein Mechanismus zur Fortsetzung eines Protokolls nach einem vollständigen oder teilweisen Verlust der Energie, und im Allgemeinen eine Sicherstellung der Integrität der Smart Card-Daten, die bei der Durchführung des Protokolls verwendet werden. Aufgrund der Risiken von Energiefluktuationen müssen üblicherweise alle Kommunikationsschritte, die von einem Protokoll für eine kontaktlose Smart Card gefordert werden, innerhalb von 150 ms durchgeführt werden. Es besteht daher ein Bedarf daran, die Zeitperiode, welche für das Protokoll zur Verfügung steht, zu erhöhen, ohne zusätzliche Risiken hinsichtlich Kommunikationsfehlern zu erzeugen.

[0004] WO-A-89/02140 (Eglise et al.) offenbart einen Mechanismus dagegen, dass eine Datenträgervorrichtung, wie eine Karte oder eine Chipkarte, aus einem Endgerät entfernt wird, bevor eine Transaktion beendet ist. Die Datenträgervorrichtung speichert einen Kreditwert, welcher unter der Kontrolle einer Maschine während des Ablaufs eines Services verringert wird. Ein derartiger Service kann ein Telefongespräch oder die Bereitstellung von Elektrizität sein. Das Problem, welches von diesem Dokument des Standes der Technik gelöst werden soll, besteht darin, sicherzustellen, dass es einem Benutzer der Datenträgervorrichtung ermöglicht ist, diese Vorrichtung zu jeder Zeit von dem Endgerät zu entfernen, ohne wichtige Kreditdaten zu verlieren, was geschehen könnte, wenn der Benutzer die Vorrichtung vor der Beendigung einer Transaktion aus dem Endgerät entfernt. Ein vergleichbarer Verlust relevanter Kreditdaten könnte auftreten, wenn die Energieversorgung vorübergehend zusammenbricht.

[0005] Um dieses Problem zu lösen, speichert die Datenträgervorrichtung nach Eglise et al. jedes Mal, wenn ein Datenkommunikationsschritt mit der Maschine durchgeführt wird, zusätzliche Informationen, welche einen Hinweis auf den betreffenden Datenkommunikationsschritt geben. Zu diesem Zweck schlagen Eglise et al. vor, zwei „Flags" und drei Parameter zu verwenden. Die Werte der Flags ändern sich entsprechend der durchgeführten Schritte, wohingegen die Parameterwerte sich entsprechend des gespeicherten Kreditwertes und dessen Aktualisierungen während aufeinander folgender Operationen ändern. Immer wenn die Datenträgervorrichtung zu früh von der Maschine entfernt wird oder wenn die Energieversorgung zusammenbricht, stellen die Werte der Flags und der Parameter, welche in dem nicht-flüchtigen Speicher der Datenträgervorrichtung gespeichert sind, einen einzigartigen Indikator des letzten durchgeführten Kommunikationsschrittes dar. Somit kann, wenn die Kommunikationen zwischen der Maschine und der Datenträgervorrichtung wieder aufgenommen werden, die vorhergehende Transaktion immer noch erfolgreich zu Ende geführt werden.

[0006] US-A-4,877,945 (Fujisaki) offenbart eine IC-Karte, welche mit einer Funktion zum Ausschließen fehlerhafter Speicherung ausgestattet ist. Die IC-Karte ist eingerichtet, um mit einem Endgerät zu kommunizieren. Zu Beginn der Kommunikation sendet das Endgerät ein Start-Kommando, wohingegen es am Ende der Kommunikation ein Ende-Kommando an die IC-Karte schickt. Nach Erhalt des Startkommandos überprüft die IC-Karte, ob ein Gültigkeits-Flag, welches in einer Tabelle in seinem EEPROM-Speicher gespeichert ist, entweder einen gültigen Status oder einen ungültigen Status indiziert. Ein ungültiger Status indiziert, dass die letzte Kommunikationsprozedur zwischen der IC-Karte und einem Endgerät nicht korrekt beendet worden ist, wohingegen ein gültiger Status darauf hinweist, dass die letzte Kommunikationsprozedur korrekt beendet worden ist.

[0007] Wenn die IC-Karte nach Erhalt eines Startkommandos erkennt, dass ihr Gültigkeits-Flag gültig ist, beginnt sie die Kommunikationsprozedur mit dem Endgerät, nachdem der Status des Gültigkeits-Flags auf „ungültig" geändert worden ist. Sie führt die Kommunikationsprozedur mit dem Endgerät durch und ändert, nach Erhalt des Endkommandos von dem Terminal, das Gültigkeits-Flag auf „gültig". Wenn jedoch die Kommunikationsprozedur vor Beendigung unterbrochen wird, verbleibt das Gültigkeits-Flag ungültig, was darauf hinweist, dass sein Dateninhalt ungültig ist.

[0008] Wenn nach Erhalt eines Startkommandos die IC-Karte erkennt, dass ihr Gültigkeits-Flag ungültig ist, informiert sie das Endgerät darüber, und es wird keine Kommunikation durchgeführt. Somit kann keine Kommunikationsprozedur durchgeführt werden, wenn eine IC-Karte ungültige Daten beinhaltet.

[0009] Um eine IC-Karte mit ungültigen Daten wieder zu verwenden, offenbart Fujisaki einen Korrekturmechanismus, welcher das Senden eines Endkommandos an die IC-Karte beinhaltet, wodurch die IC-Karte veranlasst wird, ihr Gültigkeits-Flag auf „gültig" zu ändern.

[0010] US-A-5,635,695 (Feiken) offenbart einen ähnlichen Mechanismus gegen eine Unterbrechung der Kommunikation zwischen einer IC-Karte und einem Endgerät. Feiken verwendet ebenfalls ein Gültigkeits-Flag, um auf der Karte zu indizieren, ob eine Transaktion korrekt beendet worden ist oder nicht, Darüber hinaus offenbart Feiken einen Mechanismus zur korrekten Beendigung eines unvollendeten Bilanzprozesses, nach welchem nicht nur das Gültigkeits-Flag wieder auf seinen gültigen Status gesetzt wird, sondern nach welchem auch der Dateninhalt der Karte den korrekten Wert aufweist.

[0011] WO 99/35791 offenbart ein Kommunikationssystem, welches für Kommunikationen zwischen zwei oder mehr Vorrichtungen eingerichtet ist. Die Kommunikationen basieren auf einem Transfer von Paketen. Sequenznummern werden zu den Paketen hinzugefügt. Die Sequenznummern werden in Antwort-Nachrichten von einer Vorrichtung zu einer anderen verwendet, um einen sicheren Erhalt von Paketen zu bestätigen.

Zusammenfassung der Erfindung

[0012] Eine Aufgabe der vorliegenden Erfindung besteht darin, die Zuverlässigkeit von Kommunikationen zwischen zwei Kommunikationsgeräten zu erhöhen, indem eines oder mehrere dieser Geräte gegen Fehler geschützt werden, zum Beispiel aufgrund einer Unterbrechung der Energieversorgung. Derartige Kommunikationsgeräte können eine Smart Card und ein Endgerät (Terminal) sein, können jedoch alternativ auch von jeder bekannten Art sein, zum Beispiel Computer, die miteinander über ein Netzwerk kommunizieren.

[0013] Um diese Aufgabe zu lösen, beansprucht die vorliegende Erfindung in einer ersten Ausführungsform ein Verfahren zur Kommunikation zwischen mindestens einem ersten Gerät und einem zweiten Gerät;
wobei das erste Gerät einen ersten Prozessor, erste Speichermittel und erste Eingabe/Ausgabe-Mittel umfasst, wobei die ersten Speichermittel und die ersten Eingabe/Ausgabe-Mittel mit dem ersten Prozessor verbunden sind;
wobei das zweite Gerät einen zweiten Prozessor, zweite Speichermittel und zweite Eingabe/Ausgabe-Mittel umfasst, wobei die zweiten Speichermittel und die zweiten Eingabe/Ausgabe-Mittel mit dem zweiten Prozessor verbunden sind;
wobei das Verfahren mindestens die folgenden Schritte umfasst, die von dem ersten Prozessor ausgeführt werden:

a. Ausführen eines ersten Programmschrittes in Übereinstimmung mit einem vorgegebenen ersten Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nach Ausführung des ersten Programmschritts, wobei die ersten Zustandsdaten in den ersten Speichermitteln gespeichert sind und alle Daten einschließen, die für das erste Programm erforderlich sind, um fortzufahren, wenn Instruktionen von dem zweiten Prozessor empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten einschließt, die eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
gefolgt von den folgenden Schritten mittels des zweiten Prozessors:
d. Empfangen des ersten Kommunikationsprimitivs;
e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln;
f. Ausführen eines zweiten Programmschritts in Übereinstimmung mit einem zweiten Programm;
g. Lesen der ersten zusätzlichen Daten von dem zweiten Speicher;
h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät, in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten einschließt, die eine zweite vorgegebene Beziehung mit den ersten zusätzlichen Daten aufweisen;
gefolgt von den folgenden Schritten, die von dem ersten Prozessor ausgeführt werden:
i. Empfangen des zweiten Kommunikationsprimitivs;
j. Extrahieren der zweiten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
l. Ausführen eines dritten Programmschritts in

Übereinstimmung mit dem ersten Programm.

[0014] Somit wird der Schutz gegen eine Fehlfunktion eines Geräts, beispielsweise aufgrund eines Energieverlusts, erreicht durch Anreicherung der gewöhnlichen Kommunikation zwischen den Geräten mit zusätzlichen Daten, welche im Wesentlichen dem zu schützenden Gerät gehören. Das zu schützende Gerät kommuniziert über das andere Gerät mit sich selbst, indem es die zusätzlichen Daten, die sich auf seinen eigenen inneren Zustand beziehen, transmittiert.

[0015] Der Zustand eines Gerätes umfasst alle Daten, welche erforderlich sind, dass ein Programm, welches auf dem Gerät abläuft, mit dem nächsten Programmschritt (**1**) in dem Programm fortfahren kann, nachdem es eine Antwort von dem anderen Gerät erhalten hat. Einige der Zustandsdaten können als „beständige Zustandsdaten" bezeichnet werden, d. h. als Daten, welche von dem Gerät für eine Zeitdauer gespeichert werden sollen, die sich möglicherweise über das Ende des Protokolls hinaus erstreckt, z. B. unter Verwendung eines nicht-flüchtigen Speichers, wie beispielsweise eines EEPROMs. Darüber hinaus existieren „flüchtige Zustandsdaten", welche sich auf optionale nächste Programmschritte in dem Programm, welches auf dem Gerät abläuft, beziehen. Welche Option gewählt wird, kann von den Instruktionen abhängen, welche von dem anderen Gerät empfangen werden. Das Programm erfordert die Abspeicherung dieser Zustandsdaten, um in der Lage zu sein, das Programm an seinem korrekten Punkt fortzusetzen, nachdem es Instruktionen von dem anderen Gerät erhalten hat. Üblicherweise sind die Zustandsdaten in einem flüchtigen Speicher gespeichert. Somit können diese Zustandsdaten nach einer Unterbrechung der Energieversorgung verloren gehen. Eine Unterbrechung der Energieversorgung kann insbesondere auftreten, wenn kontaktlose Smart Cards eingesetzt werden.

[0016] Das zweite Gerät extrahiert, nachdem es ein Kommunikationsprimitiv des ersten Geräts erhalten hat, die ersten zusätzlichen Daten aus dem Kommunikationsprimitiv und speichert sie in seinem eigenen Speicher. Nachdem ein nächster Programmschritt in seinem eigenen Programm ausgeführt worden ist, fügt das zweite Gerät zweite zusätzliche Daten zu einem Kommunikationsprimitiv hinzu, welches an das erste Gerät transmittiert werden soll. Die zweiten zusätzlichen Daten weisen eine vorgegebene Beziehung zu den ersten zusätzlichen Daten auf. Das erste Gerät wird die zweiten zusätzlichen Daten, welche von dem zweiten Gerät übermittelt wurden, in der nächsten Nachricht empfangen.

[0017] Die Beziehung zwischen den zweiten und ersten zusätzlichen Daten kann einfach sein: Sie können einander gleichen. Dann kann das erste Gerät die ersten zusätzlichen Daten unverändert von dem zweiten Gerät empfangen. Vorteilhaft für eine effiziente Nutzung der Kommunikationsbandbreite können jedoch die ersten zusätzlichen Daten oder Teile davon, in einer weiteren Ausführungsform, von dem zweiten Gerät zusätzlich als Eingabemedium für den in Schritt f. beschriebenen Prozessschritt eingesetzt werden. Darüber hinaus kann das zweite Gerät, zusätzlich zu einem Abspeichern der ersten zusätzlichen Daten, die ersten zusätzlichen Daten selbst verarbeiten, vorausgesetzt, dass diese Verarbeitung in verarbeiteten zweiten zusätzlichen Daten resultiert, die an das erste Gerät in dem zweiten Kommunikationsprimitiv übermittelt werden, für welches die erste Beziehung zu den ersten Zustandsdaten in dem ersten Gerät verifiziert werden kann, beispielsweise indem zunächst die Verarbeitung, welche in dem zweiten Gerät an den zusätzlichen Daten vorgenommen wurde, rückgängig gemacht wird. Die Modifikation der ersten zusätzlichen Daten kann auf diese Weise zusätzliche Informationen von dem zweiten Gerät an das erste Gerät übermitteln, was möglicherweise auch in einer effizienteren Nutzung der Kommunikationsbandbreite resultiert.

[0018] Die zusätzlichen Daten werden von dem ersten Gerät eingesetzt, um zu überprüfen, ob das auf ihm ablaufende Programm in einem korrekten Zustand wartet. Dies erfolgt durch Überprüfung, ob die empfangenen zusätzlichen Daten die vorgegebene Beziehung mit den Zustandsdaten aufweisen. Die Zustandsdaten können selbst in einem nicht-flüchtigen Teil des Speichers des ersten Gerätes gespeichert sein und werden somit sogar nach einem Ausfall der Energieversorgung vorhanden sein. Alternativ kann der nicht-flüchtige Teil des Speichers Daten speichern, von welchen diese Zustandsdaten abgeleitet werden können, wie unten erläutert werden wird.

[0019] Vorzugsweise umfasst das Verfahren in dieser ersten Ausführungsform die folgenden Schritte nach l:

m. Erstellen von zweiten Zustandsdaten, die sich auf das erste Programm beziehen, nachdem der dritte Programmschritt ausgeführt wurde;

n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät, in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv dritte zusätzliche Daten umfasst, welche eine dritte vorgegebene Beziehung zu sowohl den ersten als auch den zweiten Zustandsdaten aufweisen.

[0020] In dieser letzteren Ausführungsform umfasst das dritte Kommunikationsprimitiv nicht nur zusätzliche Daten, die eine vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen, sondern auch zu den ersten Zustandsdaten. Durch das Bereitstellen jeglicher zusätzlicher Daten mit Daten, welche eine

vorgegebene Beziehung zu allen vorhergehenden Zustandsdaten aller vorhergehenden Programmschritte in dem Programm in dem zu schützenden Gerät aufweisen, wird das Gerät in der Lage sein, das gesamte Programm nach einem Fehler in der Energieversorgung wiederherzustellen.

[0021] Dieselbe Art von Schutz kann mit dem zweiten Gerät erzielt werden. Daher bezieht sich die Erfindung in einer zweiten Ausführungsform auch auf ein Verfahren zur Kommunikation zwischen mindestens einem ersten Gerät und einem zweiten Gerät;
wobei das erste Gerät einen ersten Prozessor, erste Speichermittel und erste Eingabe/Ausgabe-Mittel umfasst, wobei die ersten Speichermittel und die ersten Eingabe/Ausgabe-Mittel mit dem ersten Prozessor verbunden sind;
wobei das zweite Gerät einen zweiten Prozessor, zweite Speichermittel und zweite Eingabe/Ausgabe-Mittel umfasst, wobei die zweiten Speichermittel und die zweiten Eingabe/Ausgabe-Mittel mit dem zweiten Prozessor verbunden sind;
wobei das Verfahren mindestens die folgenden Schritte umfasst, welche von dem ersten Prozessor ausgeführt werden:

a. Ausführen eines ersten Programmschritts in Übereinstimmung mit einem vorgegebenen ersten Programm;

b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der erste Programmschritt ausgeführt wurde, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor empfangen worden sind;

c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;

gefolgt von den folgenden Schritten mittels des zweiten Prozessors:

d. Empfangen des ersten Kommunikationsprimitivs;

e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln;

f. Ausführen eines zweiten Programmschritts in Übereinstimmung mit einem zweiten Programm und Erstellen von zweiten Zustandsdaten, welche sich auf das zweite Programm beziehen, nachdem der zweite Programmschritt ausgeführt wurde;

g. Lesen der ersten zusätzlichen Daten aus dem zweiten Speicher;

h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät, in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten umfasst, welche eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen, und dritte zusätzliche Daten, welche eine vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen; gefolgt von den folgenden Schritten, welche von dem ersten Prozessor ausgeführt werden:

i. Empfangen des zweiten Kommunikationsprimitivs;

j. Extrahieren der zweiten und dritten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv, Speichern der dritten zusätzlichen Daten in den ersten Speichermitteln und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;

k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:

l. Ausführen eines dritten Programmschritts, in Übereinstimmung mit dem ersten Programm, und Erstellen von dritten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der dritte Programmschritt ausgeführt wurde;

m. Lesen der dritten zusätzlichen Daten aus den ersten Speichermitteln;

n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät, in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv vierte zusätzliche Daten einschließt, welche eine vierte vorgegebene Beziehung zu den dritten zusätzlichen Daten aufweisen, und fünfte zusätzliche Daten, welche eine fünfte vorgegebene Beziehung zu den dritten Zustandsdaten aufweisen;

gefolgt von den folgenden Schritten, welche von dem zweiten Prozessor ausgeführt werden:

o. Empfangen des dritten Kommunikationsprimitivs;

p. Extrahieren der vierten und fünften zusätzlichen Daten aus dem dritten Kommunikationsprimitiv, Speichern der fünften zusätzlichen Daten in den zweiten Speichermitteln und Ableiten der dritten zusätzlichen Daten aus den vierten zusätzlichen Daten;

q. Überprüfen, ob die abgeleiteten dritten zusätzlichen Daten die dritte vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des zweiten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:

r. Ausführen eines vierten Programmschritts in Übereinstimmung mit dem zweiten Programm.

[0022] Die vorliegende Erfindung bezieht sich auch auf ein verteiltes Verarbeiten, in dem Sinne, dass sie nicht beschränkt ist auf Kommunikationen zwischen zwei Geräten. Sie bezieht sich auch auf Situationen, in welchen ein Prozessor Kommunikationsprimitive an einen gemeinsamen Datenspeicher oder Datenübermittlungsmittel übermittelt, wie beispielsweise einen zentralen Speicher, welcher dieses Kommunikationsprimitiv speichert. Ein Gerät aus einer Vielzahl anderer Geräte kann dieses Kommunikationsprimitiv aus dem zentralen Speicher lesen. Natürlich muss, nachdem das Kommunikationsprimitiv aus dem zentralen Speicher gelesen worden ist, ein Mechanismus existieren, um andere Geräte darüber zu informieren, dass das Kommunikationsprimitiv gelesen und verarbeitet worden ist. Dies kann dadurch erfolgen, dass das Kommunikationsprimitiv aus dem zentralen Speicher entfernt wird, nachdem es gelesen wurde. Alternativ kann jedoch das Kommunikationsprimitiv in dem zentralen Speicher gespeichert bleiben. Dann kann ein Indikator zu dem Kommunikationsprimitiv in dem zentralen Speicher hinzugefügt werden, um andere Geräte darüber zu informieren, dass das Kommunikationsprimitiv von einem Gerät gelesen worden ist und nicht von einem anderen Gerät verarbeitet werden muss.

[0023] Die Beziehung zwischen den zusätzlichen Daten und den Zustandsdaten kann darauf basieren, dass eines oder mehrere der folgenden Verfahren verwendet werden, entweder allein oder in Kombination: Anwenden eines Verschlüsselungsverfahrens, Anwenden einer kyptographischen Hash-Funktion, und Anwenden einer Verschlüsselung mit Einmal-Pad-Funktion.

[0024] Um das Verfahren in Übereinstimmung mit der ersten Ausführungsform der vorliegenden Erfindung auszuführen, bezieht sich die Erfindung auch auf ein System, wie es in dem unabhängigen Anspruch 10 beansprucht wird.

[0025] Um ein Verfahren in Übereinstimmung mit der zweiten Ausführungsform der vorliegenden Erfindung auszuführen, bezieht sich die vorliegende Erfindung auch auf ein System, wie es in dem unabhängigen Anspruch 11 beansprucht wird.

[0026] Die vorliegende Erfindung bezieht sich auch auf Geräte, welche eingerichtet sind, um miteinander zu kommunizieren, um das erfindungsgemäße Verfahren auszuführen. Daher bezieht sich die Erfindung auch auf ein Gerät, welches einen Prozessor, Speichermittel und Eingabe/Ausgabe-Mittel umfasst, wobei die Speichermittel und Eingabe/Ausgabe-Mittel mit dem Prozessor verbunden sind;
wobei der Prozessor eingerichtet ist, um mindestens die folgenden Schritte auszuführen:

a. Ausführen eines ersten Programmschritts, in Übereinstimmung mit einem vorgegebenen Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das Programm beziehen, nachdem der erste Programmschritt ausgeführt wurde, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
d. Empfangen des ersten Kommunikationsprimitivs von einem anderen Gerät;
e. Extrahieren zweiter zusätzlicher Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
f. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten eine vorgegebene Beziehung zu den Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
g. Ausführen eines zweiten Programmschritts, in Übereinstimmung mit dem Programm.

[0027] Ein derartiges Gerät kann eine Smart Card sein.

[0028] Vorzugsweise ist der Prozessor eingerichtet, um nach einer Unterbrechung und Wiederherstellung der Energieversorgung an dem Prozessor die folgenden Schritte auszuführen:
Empfangen mindestens eines Kommunikationsprimitivs von entweder dem anderen Gerät oder einem zentralen Speicher, wobei das Kommunikationsprimitiv eine vorgegebene Beziehung zu letzten Zustandsdaten aufweist, die in Übereinstimmung mit einem letzten Programmschritt erstellt wurden, der von dem ersten Programm ausgeführt worden ist;
Wiederaufnehmen des ersten Programms mit einem weiteren Programmschritt, welcher auf den letzten Programmschritt folgt.

[0029] Die vorliegende Erfindung bezieht sich auch auf ein Gerät, welches ein Terminal ist, das eingerichtet ist, um mit einer Smart Card zu kommunizieren, welches einen Prozessor umfasst, Speichermittel und Eingabe/Ausgabe-Mittel, wobei die Speichermittel und Eingabe/Ausgabe-Mittel mit dem Prozessor verbunden sind;
wobei der Prozessor eingerichtet ist, um die folgenden Schritte auszuführen:

a. Empfangen eines ersten Kommunikationsprimitivs von einem anderen Gerät;
b. Erkennen, dass das erste Kommunikationspri-

mitiv zusätzliche Daten umfasst, welche eine erste vorgegebene Beziehung zu Zustandsdaten aufweisen, die sich auf ein erstes Programm beziehen, welches auf einem anderen Gerät abläuft, wobei die ersten Zustandsdaten alle Daten umfassen, die für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem Prozessor empfangen worden sind;
c. Extrahieren der zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der zusätzlichen Daten in den Speichermitteln;
d. Ausführen eines Programmschritts, in Übereinstimmung mit dem zweiten Programm;
e. Lesen der ersten zusätzlichen Daten aus dem Speicher;
f. Übermitteln eines zweiten Kommunikationsprimitivs an das andere Gerät, in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten umfasst, welche eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen.

[0030] Die vorliegende Erfindung wird verdeutlicht unter Bezugnahme auf einige Zeichnungen, welche lediglich Verdeutlichungszwecken dienen sollen. Die vorliegende Erfindung ist in ihrem Umfang lediglich durch die angehängten Ansprüche beschränkt.

[0031] Fig. 1 zeigt eine schematische Darstellung eines Terminals und einer kontaktlosen Smart Card, welche angeordnet sind, um miteinander gemäß dem Stand der Technik zu kommunizieren;

[0032] Fig. 2 zeigt drei Geräte, welche in der Lage sind, miteinander über ein Kommunikationsnetzwerk zu kommunizieren, um die weitere Ausführungsform der vorliegenden Erfindung zu verdeutlichen;

[0033] Fig. 3a und Fig. 3b zeigen ein Flussdiagramm des erfindungsgemäßen Verfahrens in Übereinstimmung mit einem ersten Ausführungsbeispiel;

[0034] Fig. 4 zeigt einen Mechanismus, um Zustandsdaten zu erzeugen.

[0035] Fig. 1 zeigt eine Smart Card **2**, welche mit einem Mikroprozessor **6** ausgestattet ist, der mit einem Speicher **4** und einer Spule **8** verbunden ist.

[0036] Die Spule **8** dient der kontaktlosen Kommunikation mit einem anderen Gerät, wie beispielsweise einem Terminal **10**, mittels elektromagnetischer Energie, wie es Fachleuten bekannt ist. Vorzugsweise wird auch die für den Betrieb des Mikroprozessors **6** erforderliche Energie über die Spule **8** von dem anderen Gerät bereitgestellt, zum Beispiel dem Terminal **10**. Wie dies erfolgt, ist Fachleuten ebenfalls bekannt und bedarf keiner weiteren Erläuterung hier. Natürlich kann die Spule **8** ersetzt werden durch irgendeine andere Art von Schnittstellenmitteln oder Eingabe/Ausgabe-Mitteln, welche aus dem Stand der Technik bekannt sind. Die Spule **8** kann beispielsweise ersetzt werden durch elektrisch leitfähige Anschlusskontakte, mittels derer ein elektrischer Kontakt mit dem Terminal **10** hergestellt werden kann.

[0037] Der Speicher **4** ist als einzelner Block dargestellt. Der Speicher **4** wird jedoch normalerweise einen RAM (Random Access Memory, Schreib-Lese-Speicher), ROM (Read Only Memory, Festwertspeicher) und ein EEPROM (Electrically Erasable Programmable Read Only Memory, elektrisch löschbarer programmierbarer Festwertspeicher) umfassen. Diese Arten von Speichern sind Fachleuten bekannt. Falls nötig, können andere Speicherarten zu der Smart Card **2** hinzugefügt werden. Das EEPROM wird von dem Mikroprozessor eingesetzt werden, um Informationen auf der Karte **2** selbst in einer nicht-flüchtigen Art zu speichern, d. h. sie verbleiben selbst nach einem Ausfall der Energieversorgung in dem EEPROM gespeichert.

[0038] Das Terminal **10** umfasst eine Spule **14**. Die Spule **14** wird von dem Terminal **10** eingesetzt, um mit der Smart Card **2** über die Spule **8** der Smart Card **2** zu kommunizieren. Sowohl die Energie als auch Daten werden über die Spule **14** an die Smart Card **2** übermittelt, wie es Fachleuten bekannt ist. Natürlich muss, wenn die Smart Card **2** eine andere Art von Eingabe/Ausgabe-Mitteln als die Spule **8** hat, das Terminal **10** mit einer geeigneten anderen Art von Eingabe/Ausgabe-Mitteln ausgestattet sein. Daher kann die Spule **14** ersetzt werden durch eine beliebige andere Art von Eingabe/Ausgabe-Mitteln, wie sie aus dem Stand der Technik bekannt ist, z. B. Verbinder zum Herstellen eines elektrisch leitenden Kontaktes.

[0039] Der Prozessor **16** des Terminals **10** ist mit einem Speicher **18**, einem Display **22** und einer Tastatur **20** verbunden. Das Display **22** kann von einer beliebigen aus dem Stand der Technik bekannten Art sein, zum Beispiel ein Monitor oder ein LCD-Display. Die Tastatur **20** kann ersetzt werden durch eine beliebige andere Art von Eingabemitteln, um es einem Benutzer zu ermöglichen, relevante Daten einzugeben, wie beispielsweise einen Touch Screen oder eine beliebigen andere Art von Eingabemitteln, wie sie aus dem Stand der Technik bekannt sind. Die Tastatur **20** oder gleichwertige Mittel und das Display **22** können fehlen.

[0040] Vorzugsweise kann der Prozessor **16** mit anderen, entfernt angeordneten Prozessoren (nicht dargestellt) verbunden sein über eine Kommunikationslinie **17**. Dann können die entfernt angeordneten (remote) Prozessoren/der entfernt angeordnete Prozessor einen Teil des Kommunikationsprotokolls mit der Smart Card **2** ausführen. Dies ist beispielsweise

nötig, wenn die Transaktion zwischen dem Terminal **10** und der Smart Card **2** sich auf einen Abbuchungsprozess oder eine Kredittransaktion bezieht, bezüglich eines Kontos, das auf einem entfernt angeordneten Gerät verwaltet wird.

[0041] Der Speicher **18** wurde als einzelner Block dargestellt. In der Praxis wird dieser Speicher **18** jedoch verschiedene Arten von Speichern umfassen, einschließlich möglicherweise einem oder mehreren der folgenden Speicherarten: RAM, ROM, EEPROM und Festplatte. Wie in der Smart Card **2**, speichern die nicht-flüchtigen Speicherarten ausführbare Programme und andere Daten, die für die beabsichtigten Funktionen des Geräts erforderlich sind. Typischerweise dient mindestens ein Teil des Arbeitsspeichers und des nichtflüchtigen Speichertyps der ausschließlichen Benutzung durch das Gerät, während dieses Programme ausführt.

[0042] Üblicherweise erfolgt die Kommunikation zwischen dem Terminal **10** und der Smart Card **2** nicht permanent oder festgelegt und kann (re-)initialisiert werden zu jedem gewünschten Zeitpunkt. Eine derartige Situation ist typisch für Kommunikationen zwischen Smart Cards und Terminals. Jedoch können derartige Kommunikationen auch in einer Client-Server-Beziehung auftreten, zwischen Computer, die miteinander über ein Datennetzwerk, wie beispielsweise dem Internet, kommunizieren. Daher ist die vorliegende Erfindung nicht auf Smart Cards und Terminals zur Kommunikation mit Smart Cards beschränkt, sondern ist auch anwendbar auf andere Geräte, die eingerichtet sind, um miteinander zu kommunizieren. Datenkommunikationen zwischen Geräten erfolgen typischerweise als ein Austausch von Dateneinheiten, welche üblicherweise als „Pakete", „Nachrichten" oder „Kommunikationsprimitive" bezeichnet werden. Daher ist, im Zusammenhang der vorliegenden Erfindung, ein Kommunikationsprimitiv eine beliebige Art von Nachricht, welche beispielsweise Instruktionen, Aussagen und/oder Daten einschließt. Ein derartiges Kommunikationsprimitiv umfasst einen Kopf (Header) und eine Nutzlast (Payload), wie es Fachleuten bekannt ist.

[0043] Die vorliegende Erfindung ist auch anwendbar auf drei oder mehr Geräte, welche eingerichtet sind, um miteinander über ein Kommunikationsnetzwerk zu kommunizieren. Fig. 2 zeigt schematisch eine derartige Situation. Die Geräte **2** und **10** können sich auf dieselben Arten von Geräten wie in Fig. 1 beschrieben beziehen.

[0044] Gerät **26** ist eingerichtet, um mit anderen Geräten zu kommunizieren, und umfasst mindestens einen Prozessor **30**, der mit einer Schnittstelle **28** und einem Speicher **32** verbunden ist. Die Schnittstelle **28** funktioniert als das Eingabe/Ausgabe-Mittel zwischen dem Prozessor **30** und einem Kommunikationsnetzwerk **24**. Das Kommunikationsnetzwerk **24** kann beispielsweise ein PSTN (Public Switched Telephone Network, öffentlich geschaltetes Telefonnetzwerk) oder eine beliebige andere Art von Kommunikationsnetzwerk sein, entweder WAN (Wide Area Network, Weitverkehrsnetz) oder LAN (Local Area Network, lokales Netzwerk), oder eine andere Art. Es kann auch das Internet sein. Die Schnittstelle **28** kann von beliebiger Art sein, wie sie den Fachleuten bekannt ist.

[0045] Der Speicher **32** wurde als einzelner Block dargestellt. In der Praxis wird der Speicher **32** ein RAM, ROM, EEPROM oder eine beliebige andere Art von Speicher umfassen, entweder allein oder in Kombination, wie es Fachleuten bekannt ist. Sie können in einer oder mehreren physikalischen Einheiten realisiert sein.

[0046] Wie unten erläutert werden wird, kann zur Implementierung einer speziellen Ausführungsform der vorliegenden Erfindung ein zentraler Speicher **34** vorliegen, welcher für jedes der Geräte **2**, **10**, **26** über das Netzwerk **24** zum Speichern und Extrahieren von Daten zugänglich ist. Der zentrale Speicher **34** kann mit Intelligenz (nicht dargestellt) ausgestattet sein, um Speicher-, Lese- und Lösch-Vorgänge auszuführen, wie es Fachleuten bekannt ist. Somit kann der zentrale Speicher **34** Teil eines gemeinsamen (shared) Datenspeichers oder von Datenübertragungsmitteln sein.

[0047] Das Netzwerk **24**, welches die Geräte **2**, **10**, **26** verbindet, kann öffentlich zugänglich sein, in dem Sinn, dass viele Geräte gleichzeitig das Netzwerk nutzen können, unter Verwendung einer beliebigen bekannten Netzwerk-Zuordnungs-Prozedur, um eine Kommunikation in einer pseudo-privaten Weise durchzuführen. Ein Teilen des Netzwerks ermöglicht eine Teilung der Datenkommunikation zwischen beliebigen der anderen Geräte, welche mit dem Netzwerk verbunden sind. Daher existiert, wenn ein gemeinsames Netzwerk verwendet wird, die Privatsphäre der kommunizierten Daten sowie des Kommunikationsschemas nicht tatsächlich. Dann muss, falls dies erforderlich ist, die Privatsphäre der Nutzer der Geräte bereitgestellt werden mittels anderer Mittel, was oft eine Verschlüsselung einschließt. Andererseits ermöglicht die Teilung der Datenkommunikation zwischen beliebigen der Geräte, welche mit dem gemeinsamen Netzwerk verbunden sind, dass die Kommunikation zwischen diesen Geräten, welche mit den Medien verbunden sind, tatsächlich durch eine Anzahl physikalisch unterschiedlicher Geräte durchgeführt wird, welche für den Zweck einer speziellen Kommunikation als ein einziges „logisches" Gerät zusammenarbeiten.

[0048] Ein Gerät oder in gleicher Weise eine Sammlung von zusammenarbeitenden Geräten nehmen an

der Kommunikation entweder in der Rolle eines Initiators, im Allgemeinen als der „Klient" bezeichnet, oder in der Rolle eines Antwortenden, im Allgemeinen als der „Server" bezeichnet, teil. Folglich wird eine spezielle Sequenz von Nachrichten zwischen dem Klienten und dem Server ausgetauscht, um einen „Service" bereitzustellen, welcher von dem Server an den Klienten geliefert wird. In der in Fig. 1 gezeigten Anordnung ist das Terminal **10** der Klient, wohingegen die Smart Card **2** der Server ist.

[0049] Das System kommunizierender Geräte kann auch Geräte einschließen, welche als getrennte Prozesse realisiert sind, oder Kontrollpfade, auf einem einzelnen Computer, welcher über einen gemeinsamen Speicher kommuniziert.

[0050] Die Datenkommunikation zwischen derartigen Geräten beliebiger Art und Struktur wird üblicherweise auf eine geordnete Art durchgeführt, mit einer Sequenz von Nachrichten, welche zwischen den Geräten ausgetauscht werden, beginnend mit einer anfänglichen Nachricht von dem Klienten. Für den Zweck der Kommunikation sind die Nachrichten oder Kommunikationsprimitive identifizierbar durch den empfangenden Teilnehmer, wie dies in der geordneten Sequenz von Nachrichten geeignet ist.

[0051] Jede Nachricht oder jedes Kommunikationsprimitiv, welche empfangen werden, übermitteln Informationen, welche für das empfangende Gerät erforderlich sind, um einen einzelnen Schritt hin zum Ziel der Kommunikationssequenz fortzuschreiten. Zu diesem Zweck implementiert das empfangende Gerät in irgendeiner Weise Funktionen, welche üblicherweise als „Zustandsmaschine" bekannt sind, um zu erkennen, dass das empfangene Kommunikationsprimitiv in die Sequenz passt, und, wenn dies zweckdienlich ist, um die Daten in dem Kommunikationsprimitiv weiter zu interpretieren. Die Zustandsmaschine umfasst im Allgemeinen ausführbare Befehle und beschreibende Daten, welche in dem Speicher des Gerätes gespeichert sind, welche in Kombination beschreiben:

(1) welche Nachricht zu erwarten ist;
(2) die Art, auf welche beliebige Daten, die in der Nachricht enthalten sind, verarbeitet werden sollen; und
(3) welche Nachricht als Antwort gesendet werden soll.

[0052] Insbesondere kann der Arbeitsspeicher des empfangenden Gerätes derartige beschreibende Daten umfassen, welche sofort aktualisiert werden können, bevor eine Nachricht in ihrer Gesamtheit an das andere Gerät gesendet worden ist, um den Fortschritt widerzuspiegeln, welcher in der geordneten Sequenz der Nachrichten erzielt worden ist. Der Arbeitsspeicher des empfangenden Geräts kann auch die Resultate der Verarbeitung der empfangenen Nachrichtendaten umfassen, zum Beispiel ein Modifizieren oder Abspeichern beliebiger Daten, welche in den Nachrichten empfangen worden sind. Derartige beschreibende Daten in dem Arbeitsspeicher werden üblicherweise als „Zustandsdaten" oder kurz „Zustand" bezeichnet.

[0053] Alle logischen Geräte **2**, **10**, **26**, die in Übereinstimmung mit der vorliegenden Erfindung mittels eines geordneten Austausches von Kommunikationsprimitiven kommunizieren, halten jeweils in den Speichern **4**, **18**, **32** Daten aufrecht, welche den Zustand der Kommunikation definieren.

[0054] Die Zustandsdaten werden üblicherweise in flüchtigem Speicher gespeichert. Daher ist es nach einem Ausfall der Energieversorgung nicht sicher, dass die Zustandsdaten in dem flüchtigen Speicher immer noch gültig sind. Sie können teilweise oder vollständig verloren gegangen sein. Um zu bestätigen, dass die Zustandsdaten in dem Arbeitsspeicher immer noch gültig sind, nachdem das Gerät ein nächstes Kommunikationsprimitiv des anderen Gerätes empfangen hat, schlägt die vorliegende Erfindung ein spezielles Verfahren vor, welches im Folgenden erläutert werden wird. Es sei darauf hingewiesen, dass das Verfahren auch gegen teilweisen oder vollständigen Verlust von Zustandsdaten aufgrund von anderen Ursachen als einem Ausfall der Energieversorgung schützt.

[0055] In Übereinstimmung mit der vorliegenden Erfindung umfasst in dem beschriebenen System und dem Verfahren mindestens eines der Kommunikationsgeräte zusätzliche Daten in mindestens einem der Kommunikationsprimitive, welches es an das andere Gerät sendet. Diese zusätzlichen Daten repräsentieren den inneren Zustand, wie er allgemein beschrieben wird, durch die Daten, die in seinem Arbeitsspeicher abgespeichert sind. Dies wird weiter verdeutlicht unter Bezugnahme auf die Fig. 3a und Fig. 3b. In den Fig. 3a und Fig. 3b wird ein Kommunikationsverfahren zwischen zwei Geräten gemäß der Erfindung verdeutlicht, d. h. einem Gerät A (dem Server, beispielsweise einer Smart Card **2**) und einem Gerät B (dem Klienten, beispielsweise dem Terminal **10**).

[0056] Gerät A ist typischerweise ein Server, welcher Zustandsdaten aufrechterhalten muss, die sich auf die empfangenen Nachrichten beziehen, und auf die Daten, welche diese Nachrichten enthalten. Insbesondere kann jeder Sicherheitsstatus, wie beispielsweise eine Authentifizierung oder ein temporär eingerichteter Verschlüsselungs-Schlüssel, welche von dem Klienten im Laufe des derzeitigen Austauschs von Kommunikationsprimitiven erhalten wurden, Teil der Server-Zustandsdaten sein.

[0057] Gerät B ist typischerweise ein Klient und um-

fasst typischerweise spezielle Verarbeitungs-Instruktionen, um ein derartiges Kommunikationsprimitiv zu handhaben, welches derartige zusätzliche Daten umfasst. Insbesondere wird der Klient, als Teil der Verarbeitung des empfangenen Kommunikationsprimitivs, die zusätzlichen Daten aus dem Kommunikationsprimitiv extrahieren, wie im Folgenden erläutert werden wird.

[0058] Der Kommunikationsprozess startet, indem Gerät B eine Kommunikationsanfrage an Gerät A schickt, um ein vorgegebenes Protokoll mit dem Gerät A auszuführen (Schritt **200**).

[0059] In Schritt **100** empfängt Gerät A die Kommunikationsanfrage von Gerät B und startet die Kommunikation.

[0060] Der nächste Schritt, Schritt **102**, dient dazu, einen ersten Programmschritt auszuführen, in Übereinstimmung mit einem vorgegebenen Programm, in Antwort auf die Kommunikationsanfrage, die von dem Gerät B empfangen wurde.

[0061] Nach Ausführung des ersten Programmschritts speichert Gerät A in seinem Arbeitsspeicher Zustandsdaten, welche sich auf den Punkt in dem Programm beziehen, an dem das Programm warten muss auf weitere Daten und/oder Instruktionen des Geräts B, oder Daten, aus welchen die Zustandsdaten abgeleitet werden können, Schritt **104**.

[0062] In Schritt **106** sendet Gerät A, um die geeignete Eingabe von Gerät B zu empfangen, ein Kommunikationsprimitiv, einschließend zusätzliche Daten, welche eine vorgegebene Beziehung zu seinen eigenen Zustandsdaten aufweisen, an Gerät B.

[0063] In Schritt **202** empfängt Gerät B die Nachricht von Gerät A.

[0064] In Schritt **204** überprüft Gerät B, ob die empfangene Nachricht Prozess-Ende-Instruktionen umfasst. Ist dies der Fall, so springt Gerät B zum Ende seines Programms (Schritt **218**). Ist dies nicht der Fall, so schreitet Gerät B mit Schritt **206** fort, in welchem Gerät B die zusätzlichen Daten hinsichtlich der Zustandsdaten des Gerätes A aus der empfangenen Nachricht extrahiert.

[0065] In Schritt **208** speichert Gerät B diese zusätzlichen Daten in seinem Speicher **18**, vorzugsweise ohne diese zusätzlichen Daten zu verarbeiten.

[0066] In Schritt **210** führt Gerät B einen nächsten Programmschritt aus, in Übereinstimmung mit seinem eigenen Programm.

[0067] In Schritt **212** speichert Gerät B Zustandsdaten, welche sich auf seinen eigenen Prozess beziehen, in seinem Speicher **18**.

[0068] In Schritt **214** liest Gerät B die zusätzlichen Daten, welche sich auf die Zustandsdaten des Gerätes A beziehen, welche in dem Speicher **18** in Schritt **208** gespeichert wurden, aus dem Speicher **18** aus.

[0069] In Schritt **216** sendet Gerät B ein Kommunikationsprimitiv, welches mindestens diese letzteren zusätzlichen Daten umfasst, an Gerät A. Dieses Kommunikationsprimitiv kann weiterhin Instruktionen umfassen, welche von dem Gerät A ausgeführt werden sollen.

[0070] In Schritt **217** überprüft Gerät B, ob sein Prozess sein Ende erreicht hat. Ist dies der Fall, so springt es zu Schritt **218** (Ende). Ist dies nicht der Fall, so springt es zurück zu Schritt **202** und wartet auf weitere Nachrichten von Gerät A.

[0071] In Schritt **108** empfangt Gerät A das Kommunikationsprimitiv von Gerät B.

[0072] In Schritt **110** extrahiert das Gerät A die zusätzlichen Daten, welche sich auf die Zustandsdaten des Gerätes A beziehen, aus dem empfangenen Kommunikationsprimitiv.

[0073] In Schritt **112** überprüft Gerät A, ob die extrahierten zusätzlichen Daten korrekt sind. Dies kann auf verschiedene Weisen erfolgen. Beispielsweise kann Gerät A, wenn es seine letzten gültigen Zustandsdaten in dem Speicher abgespeichert hat, einfach die extrahierten zusätzlichen Daten mit diesen gespeicherten Daten vergleichen, um zu überprüfen, ob diese gleich sind. Alternativ kann das Gerät A auch Daten abgespeichert haben, aus welchen die letzten gültigen Zustandsdaten auf eindeutige Weise abgeleitet werden können. Ein Beispiel wird unten aufgeführt, unter Bezugnahme auf Fig. 4. Dann muss das Gerät A die letzten gültigen Zustandsdaten zunächst aus diesen gespeicherten Daten ableiten, wonach ein Vergleich mit den extrahierten zusätzlichen Daten durchgeführt werden kann.

[0074] Wenn die Überprüfung positiv verläuft, wird es Gerät A erlaubt, das laufende Programm fortzusetzen. Dann schreitet es fort mit Schritt **120**, über den Schritt **114**. Wenn jedoch festgestellt wird, dass der Überprüfungsschritt **112** kein positives Resultat ergibt, so ist irgendwo ein Fehler aufgetreten. Ein derartiger Fehler kann durch verschiedene Umstände entstehen. Beispielsweise kann ein Fehler in der Energieversorgung für Gerät A aufgetreten sein, was in einem teilweisen oder vollständigen Verlust der Zustandsdaten resultiert, welche in dem Speicher **8** gespeichert sind. Ein anderer Grund kann darin liegen, dass die empfangenen zusätzlichen Daten versehentlich oder absichtlich verändert worden sind. Unabhängig von dem Grund dafür, dass der überprüfte

Prozess negativ ist, kann das Programm in Gerät A nicht einfach mit dem Ablauf fortfahren. Nun können zwei verschiedene Schritte durchgeführt werden. Entweder führt Gerät A, nachdem es möglicherweise Gerät B mittels einer Warnnachricht darüber informiert hat, dass ein Fehler aufgetreten ist (Schritt **116**), einen Wiederherstellungsprozess aus (Schritt **118**), oder es springt zum Ende seines Programms (in Fig. 3b nicht gezeigt).

[0075] Der Wiederherstellungsprozess (Schritt **118**) ist möglich, wenn die zusätzlichen Daten, welche von dem Gerät B empfangen worden sind, genügend und verlässliche Informationen für das Gerät A umfassen, um daraus alle notwendigen Zustandsdaten abzuleiten, um sein Programm an dem Punkt fortzusetzen, an welchem der letzte Programmschritt ausgeführt wurde, bevor auf weitere Eingaben von Gerät B gewartet wurde. Nach einem korrekten Wiederherstellungsprozess, was in Schritt **119** überprüft wird, kann das Programm mit Schritt **120** fortfahren. Wenn die Wiederherstellung nicht erfolgreich war, kann eine dementsprechende Nachricht erzeugt werden und an Gerät B übermittelt werden (Schritt **121**), und das Programm endet (Schritt **126**).

[0076] In Schritt **120** führt Gerät A einen nächsten Programmschritt aus, in Übereinstimmung mit seinem eigenen Programm.

[0077] In Schritt **122** speichert Gerät A wiederum, nachdem es den nächsten Programmschritt ausgeführt hat, die derzeit gültigen Zustandsdaten in seinem Speicher **8**, oder Daten, aus welchen die Zustandsdaten abgeleitet werden können.

[0078] Wenn, wie in Schritt **124** angedeutet, festgestellt wird, dass das Programm beendet werden kann, geht es zu Schritt **126**. Andernfalls wird das Programm mit Schritt **106** fortgesetzt, um einen neuen Zyklus zu starten, in Übereinstimmung mit der vorliegenden Erfindung. Nach Schritt **126** kann das Programm mit Schritt **100** fortfahren.

[0079] Während des Wiederherstellungsschritts **118** wird das Gerät A überprüfen, ob die empfangenen zusätzlichen Daten von Gerät B verbunden sind mit einem Zustand an einem Punkt in seinem Programm, an welchem es sich nun befinden könnte, wenn kein Fehler aufgetreten wäre, oder ob dies nicht der Fall ist. In den meisten Fällen wird dies lediglich möglich sein, wenn das Gerät A einige relevante Daten in seinem nicht-flüchtigen Speicherteil gespeichert hat, welche immer noch vorhanden sind nach dem Ausfall der Energieversorgung. Diese relevanten Daten in dem nicht-flüchtigen Speicherteil müssen nicht umfangreich sein. Die meisten der Daten können in dem flüchtigen Speicherteil des Speichers **8** gespeichert sein und können zurückerhalten werden von Gerät B im nächsten Kommunikationsprimitiv, zum Beispiel enthalten in den zusätzlichen Daten.

[0080] Der Wiederherstellungsprozess kann leicht umgesetzt werden, wenn das Gerät A die zusätzlichen Daten zu irgendeiner Zeit generiert, derart, dass sie eine vorgegebene Beziehung nicht nur zu den letzten Zustandsdaten in dem laufenden Programm aufweisen, sondern auch zu allen vorhergehenden Zustandsdaten. Dann ist es einfacher für das Gerät A, zu bestimmen, welche Programmschritte in dem Programm bereits ausgeführt worden sind, und somit, welche Zustände in der Vergangenheit schon erreicht worden sind.

[0081] Die Erfindung ist nicht beschränkt auf die Erzeugung derartiger zusätzlicher Daten mit einer vorgegebenen Beziehung zu den Zustandsdaten in Gerät A. Sie ist auch anwendbar auf Gerät B. Somit kann auch Gerät B mit der Option ausgestattet sein, zusätzliche Daten, die sich auf die Zustandsdaten des laufenden Programms auf Gerät B beziehen, zu generieren. Derartige zusätzliche Daten, die von Gerät B erzeugt werden, werden an das Gerät A mit dem nächsten Kommunikationsprimitiv übermittelt und werden von Gerät A aus jedem Kommunikationsprimitiv extrahiert. Nachdem jegliche Instruktionen ausgeführt worden sind, wird Gerät A weitere zusätzliche Daten einfügen, welche eine vorgegebene Beziehung zu (z. B. können diese gleich sein mit) den zusätzlichen Daten haben, die von Gerät B empfangen werden, in ein nächstes Kommunikationsprimitiv einfügen, welches an Gerät B übermittelt werden soll. Dann hat Gerät B denselben Grad an Schutz wie Gerät A.

[0082] Sowohl für Gerät A als auch für Gerät B weisen die zusätzlichen Daten, so wie sie erzeugt worden sind, eine vorgegebene Beziehung zu allen vorhergehenden Zustandsdaten innerhalb der jeweiligen Geräte A und B auf.

[0083] In der Erläuterung der Fig. 3a und Fig. 3b, wie sie oben gegeben wurde, war eine einfache Beziehung zwischen den zusätzlichen Daten, die von Gerät B empfangen wurden und später an Gerät A zurückübermittelt wurden, angenommen worden: Sie können einander gleich sein. Dann empfangt Gerät A die zusätzlichen Daten unverändert vom Gerät B. Vorteilhaft für eine effiziente Nutzung der Kommunikationsbandbreite können die zusätzlichen Daten oder Teile davon in einer weiteren Ausführungsform auch von Gerät B als Eingabemedium für den Verarbeitungsschritt, der in Schritt **210** beschrieben wurde, genutzt werden. Darüber hinaus kann Gerät B, zusätzlich zu einem Abspeichern der empfangenen zusätzlichen Daten, die empfangenen zusätzlichen Daten selbst verarbeiten, vorausgesetzt, dass dieses Verarbeiten in verarbeiteten neuen zusätzlichen Daten resultiert, die an das Gerät A übermittelt werden, für welche die Beziehung zu den Zustandsdaten in

Gerät A durch Gerät A verifiziert werden kann, z. B. indem zunächst die Verarbeitung der zusätzlichen Daten, die in Gerät B erfolgt ist, rückgängig gemacht wird. Diese Modifikation der zusätzlichen Daten kann auf diese Weise überschüssige Informationen von dem zweiten Gerät an das erste Gerät übermitteln, was möglicherweise auch in einer effizienteren Nutzung der Kommunikationsbandbreite resultiert.

[0084] Die vorliegende Erfindung ist auch anwendbar auf eine verteilte Umgebung, wie sie in Fig. 2 dargestellt ist. Dann kann das Gerät A beispielsweise eine Smart Card **2** sein. Anstelle einer direkten Kommunikation aller Kommunikationsprimitive an ein Gerät B kann Gerät A jedoch tatsächlich auch seine Kommunikationsprimitive zunächst an einen zentralen Speicher **34** übermitteln. Zwei oder mehr Geräte **10**, **26** sind angeordnet, um, zu Zeiten, wenn diesen Arbeitszeit zur Verfügung steht, auf dem zentralen Speicher **34** zu überprüfen, ob der zentrale Speicher **34** ein zu verarbeitendes Kommunikationsprimitiv umfasst oder nicht. Eine Option besteht darin, dass ein derartiges Gerät **10**, **26** ein vorliegendes Kommunikationsprimitiv aus dem zentralen Speicher **34** ausliest und das Kommunikationsprimitiv anschließend aus dem zentralen Speicher **34** entfernt. Somit kann es vermieden werden, dass ein anderes Gerät ebenfalls das Kommunikationsprimitiv aus dem zentralen Speicher **34** liest, um es zu verarbeiten.

[0085] Eine andere Option besteht darin, dass das Gerät, welches ein derartiges Kommunikationsprimitiv, das in dem zentralen Speicher **34** vorliegt, gelesen hat, einen Identifikator, wie beispielsweise ein Flag, zu dem Kommunikationsprimitiv in dem zentralen Speicher **34** hinzufügt, welcher anzeigt, dass das Kommunikationsprimitiv schon von einem der Geräte **10**, **26** gelesen worden ist und nicht mehr von einem anderen Gerät verarbeitet werden muss. Dann wird der zentrale Speicher **34** alle Kommunikationsprimitive während eines Protokolls sammeln. Wenn diese Kommunikationsprimitive sich alle auf einzelne Zustandsdaten des Programms, das in Gerät **2** ausgeführt worden ist, beziehen, so kann das Gerät **2** nach einem Ausfall der Energieversorgung oder einer anderen Fehlfunktion alle Kommunikationsprimitive aus dem zentralen Speicher **34** einsammeln, um den unterbrochenen Prozess wiederherzustellen. Natürlich ist es in der Ausführungsform, in welcher jedes Kommunikationsprimitiv alle relevanten Daten von allen vorhergehenden Zustandsdaten des Prozesses in dem Gerät **2** umfasst, nicht erforderlich, alle nachfolgenden Kommunikationsprimitive abzuspeichern, sondern lediglich das letzte Kommunikationsprimitiv im Speicher zu behalten.

[0086] Manchmal kann nach einer Unterbrechung der Energieversorgung und einer Wiederherstellung das Gerät **2** einfach Gerät **10** auffordern, das letzte Kommunikationsprimitiv noch einmal zu übermitteln, und Gerät **2** kann in der Lage sein, den Ablauf seines Programms wieder aufzunehmen.

[0087] Vorzugsweise umfasst das Kommunikationsprimitiv Identifikationsdaten zum Identifizieren, dass die Kommunikationsprimitive zusätzliche Daten umfassen, welche sich auf Zustandsdaten in einem der Geräte **2**, **10**, **26** beziehen.

[0088] Wie unten erläutert werden wird, kann die Beziehung zwischen den zusätzlichen Daten und den Zustandsdaten darauf basieren, dass eine Verschlüsselungstechnologie, kryptographische Hash-Funktionen (Einmal-Funktionen) und Verschlüsselung mit einem Einmal-Pad verwendet werden.

[0089] Die einfachste Beziehung zwischen den zusätzlichen Daten und den Zustandsdaten ist eine Eins-zu-eins-Beziehung, d. h. die zusätzlichen Daten entsprechen den Zustandsdaten, welche nach dem letztem Programmschritt, der von dem Programm ausgeführt worden ist, gültig sind. Jedoch sind in den meisten Fällen die Zustandsdaten vertraulich und dürfen nur dem betroffenen Gerät bekannt sein. Dann dürfen die zusätzlichen Daten die Zustandsdaten nicht an die Umgebung preisgeben, und ein Schutz gegen eine Aufdeckung dieser Zustandsdaten muss vorgesehen sein.

[0090] Eine Option zum Schutz der Zustandsdaten besteht darin, diese mit einem Verschlüsselungs-Schlüssel zu verschlüsseln, welcher nur dem Gerät bekannt ist, welches sich auf die Zustandsdaten bezieht. Der verschlüsselte Zustand wird dann als die zusätzlichen Daten in dem Kommunikationsprimitiv an das andere Gerät (oder an den zentralen Speicher **34**) übermittelt. Das Gerät speichert die Zustandsdaten (oder andere Daten, aus welchen die Zustandsdaten direkt abgeleitet werden können) in seinem Arbeitsspeicher. Nachdem das nächste Kommunikationsprimitiv des anderen Gerätes empfangen worden ist, überprüft das Gerät, ob die zusätzlichen Daten, welche von dem anderen Gerät empfangen worden sind, gleich der verschlüsselten Form der Zustandsdaten sind. Zu diesem Zweck entschlüsselt es die empfangenen zusätzlichen Daten und vergleicht die entschlüsselten zusätzlichen Daten mit den gespeicherten Zustandsdaten. Alternativ kann es auch seine gespeicherten Zustandsdaten verschlüsseln und das Resultat mit den empfangenen zusätzlichen Daten vergleichen.

[0091] Sowohl in Fällen, in welchen die zusätzlichen Daten die Zustandsdaten selbst umfassen, als auch in Fällen, in welchen sie verschlüsselte Zustandsdaten umfassen, kann eine Verwendung eines kryptographischen Hash (Einmal-Funktion) die Sicherheit weiter erhöhen. Ein derartiger kryptographischer Hash wird von dem Gerät generiert, welches den Zu-

standsdaten zugeordnet ist, vorzugsweise unter Verwendung eines kryptographischen Schlüssels, welcher vorzugsweise lediglich dem Gerät bekannt ist, in einer Weise, wie sie Fachleuten bekannt ist. Ein derartiger Hash wird zu den zusätzlichen Daten hinzugefügt und verändert diese nicht. Der Hash hat jedoch eine vorgegebene Beziehung zu dem Inhalt der zusätzlichen Daten. Daher wird, wenn der Inhalt der zusätzlichen Daten versehentlich oder mit Absicht verändert worden ist, dies direkt erkannt werden, indem die Beziehung zwischen dem Hash und dem Inhalt der veränderten zusätzlichen Daten überprüft wird. Indem ein derartiger Hash verwendet wird, kann das Gerät, nachdem es die zurückgekehrten zusätzlichen Daten mit dem Hash empfangen hat, nicht nur die Gültigkeit der zurückgekehrten zusätzlichen Daten überprüfen, sondern kann diese auch verwenden, um die Zustandsdaten daraus abzuleiten, wenn sein eigener Zustand teilweise oder vollständig verloren gegangen ist. Ein derartig abgeleiteter Zustand kann genutzt werden, um ein Programm wieder aufzunehmen, welches zum Beispiel aufgrund eines Fehlers in der Energieversorgung unterbrochen worden ist.

[0092] Vorteilhafterweise wird der kryptographische Schlüssel, welcher entweder als Verschlüsselungs-Schlüssel oder als Hash-Schlüssel eingesetzt wird, abgeleitet aus einem Zufalls- oder Pseudo-Zufalls-Wert, welcher beispielsweise erzeugt wird, wenn das Gerät sein erstes Kommunikationsprimitiv empfängt. Dieser (Pseudo-)Zufalls-Wert kann eine Beziehung zu dem Inhalt des empfangenen Kommunikationsprimitivs aufweisen. Das Gerät speichert diesen (Pseudo-)Zufalls-Wert in seinem nicht-flüchtigen Speicherteil, bevor ein Antwort-Kommunikationsprimitiv an das andere Gerät gesendet wird.

[0093] Der (Pseudo-)Zufalls-Wert kann eingesetzt werden als Wert, aus welchem Zustandsdaten abgeleitet werden können. Alternativ kann er verwendet werden als kryptographischer Schlüssel, entweder für den Verschlüsselungsprozess oder für den Hash-Prozess oder beide. Darüber hinaus verändert sich, in einer weiteren Ausführungsform, der kryptographische Schlüssel jedes Mal, wenn eine Verschlüsselung oder ein Hash-Prozess eingesetzt wird, was die Sicherheit weiter fördert. Natürlich muss dann, jedes Mal, wenn ein neuer kryptographischer Schlüssel verwendet wird, sein Wert in dem nicht-flüchtigen Teil des Speichers gespeichert werden. Jedes beliebige Verfahren der Generierung aufeinander folgender kryptographischer Schlüssel kann eingesetzt werden. Beispielsweise kann ein neuer Schlüssel erzeugt werden durch eine Kombination zwischen einem existierenden Schlüssel und irgendeinem Inhalt eines empfangenen Kommunikationsprimitivs, oder indem zwei frühere Schlüssel in einer spezifischen Weise kombiniert werden. Die Verwendung von Einmal-(Hash-)Funktionen kann jedoch vorteilhaft eingesetzt werden, wie unten näher erläutert wird, unter Bezugnahme auf Fig. 4.

[0094] Fig. 4 zeigt ein Flussdiagramm der Verwendung einer (Pseudo-)Zufalls-Zahl, welche eingesetzt wird, um Zustandsdaten abzuleiten, nachdem eine Antwortnachricht empfangen worden ist. Nach dem Start, Schritt **300**, generiert das betroffene Gerät in Schritt **302** die (Pseudo-)Zufalls-Zahl, welche in dem nicht-flüchtigen Speicher gespeichert werden kann. Dies kann auf eine beliebige Weise erfolgen, welche Fachleuten bekannt ist. Das Gerät wendet eine Einmal-Funktion n-mal auf diese Zufallszahl an, Schritte **304(l)** bis **304(n)**, wobei n einen vorgegebenen Wert größer 0 aufweist. Beispielsweise kann anfänglich n = 10 sein. Die Verwendung von Einmal-Funktionen ist im Stand der Technik bekannt und bedarf keiner weiteren Erläuterung hier.

[0095] Das Resultat des Schritts **304(n)** wird als zusätzliche Daten in der nächsten Nachricht von dem Gerät an ein anderes Gerät (oder an den Speicher **34**) übermittelt, Schritt **306**. In Schritt **308** wartet das Gerät auf eine Antwortnachricht.

[0096] Nachdem eine derartige Antwortnachricht empfangen worden ist, extrahiert das Gerät die zusätzlichen Daten aus der Antwortnachricht, Schritt **310**. In Schritten **312** bis **320** wendet das Gerät die Einmal-Funktion auf die Zufallszahl an, welche in dem nicht-flüchtigen Speicher gespeichert ist, so oft, bis das erhaltene Resultat den extrahierten zusätzlichen Daten entspricht. Wenn keine Fehler aufgetreten sind, so wird dies beim ersten Mal n-mal sein. Dann weiß das Programm, dass der letzte Programmschritt, der ausgeführt worden ist, sich auf den ersten möglichen Zustand bezog, und das Programm wird fortgesetzt mit der Zustandszahl 1, Schritt **324**. Wenn, nachdem die Einmal-Funktion n-mal auf die Zufallszahl angewandt worden ist, immer noch keine Übereinstimmung erreicht worden ist, ist ein Fehler aufgetreten, und das Programm wird fortgesetzt mit einer Fehlerroutine, Schritt **322**.

[0097] Dann wird, um den nächsten Schritt vorzubereiten, 1 von n abgezogen, Schritt **326**, und der Prozess wird mit Schritt **304(l)** fortgesetzt. In einer bevorzugten Ausführungsform wird das Resultat dieses Schritts jedoch dadurch erhalten, dass der erforderliche Wert aufgegriffen wird, während die Iteration in Schritt **318** durchgeführt wird, wie es Fachleuten bekannt ist. Somit erfolgt für jeden nächsten Zustand in dem Programm die Anwendung der Einmal-Funktion auf die Zufallszahl um 1 weniger als in dem vorhergehenden Schritt. Da eine Einmal-Funktion eingesetzt wird, stellt dies sicher, dass ein anderes Gerät niemals in der Lage sein wird, die nächsten zusätzlichen Daten, welche sich auf den nächsten Zustand beziehen, abzuleiten: Vorausgesetzt, andere Geräte kennen nicht die (Pseudo-)Zufalls-Zahl, welche in Schritt **302** durch die fundamentale Eigenschaft kryptogra-

phischer Einmal-Funktionen erzeugt worden ist, ist es nicht möglich, die von dem Gerät durchgeführte Berechnung umzukehren und auf diese Weise Daten für den nächsten Zustand vorherzusagen.

[0098] Fig. 4 bezieht sich auf eine Situation, in welcher die gespeicherte Zufallszahl und die Einmal-Funktion eingesetzt werden, um die korrekte Zahl des letzten erreichten Zustands in dem Programm abzuleiten. Ein ähnliches oder identisches Schema kann jedoch eingesetzt werden, um einen Schlüssel zu erzeugen, welcher in einem Verschlüsselungsprozess oder einem Hash-Prozess eingesetzt werden soll.

[0099] In einem Hash-Prozess wird beispielsweise das Resultat von Schritt **304(n)** nicht direkt als zusätzliche Daten in der nächsten Nachricht gesendet, sondern dieses Resultat wird als ein Schlüssel eingesetzt, um einen authentifizierenden Hash über alle Zustandsdaten, die in der nächsten Nachricht übermittelt werden sollen, zu berechnen. Dies kann vorteilhafterweise erfolgen, wenn die Zustandsdaten mehr Informationen umfassen als lediglich eine Zahl des betroffenen Zustandes. Dann wird, nachdem die nächste Antwortnachricht empfangen worden ist und nachdem die zusätzlichen Daten aus der nächsten Antwortnachricht extrahiert worden sind, der Hash verwendet, um die Korrektheit der zurückgekehrten Zustandsdaten zu überprüfen. Dieser überprüfte Zustand wird eingesetzt, um das Programm fortzusetzen. Wiederum kann die Anzahl, wie oft die Einmal-Funktion auf die gespeicherte Zufallszahl angewandt wird, um bei einem in der Hash-Funktion einzusetzenden Schlüssel anzulangen, für jeden nächsten zu übermittelnden Zustand um 1 reduziert werden. Der in jedem Übermittlungsschritt eingesetzte Schlüssel kann in einem nicht-flüchtigen Speicherteil des Speichers gespeichert werden, es ist jedoch nicht erforderlich, den Schlüssel abzuspeichern, da er aus der gespeicherten Zufallszahl und der verwendeten Einmal-Funktion abgeleitet werden kann.

[0100] In einem Verschlüsselungsverfahren wird das Resultat des Schritts **304(n)** nicht direkt als zusätzliche Daten in der nächsten Nachricht gesendet, sondern dieses Resultat wird verwendet als Schlüssel, um alle Zustandsdaten, die in der nächsten Nachricht übermittelt werden sollen, zu verschlüsseln. Dies kann vorteilhafterweise erfolgen, wenn die Zustandsdaten nicht an externe Geräte weitergegeben werden dürfen. Dann werden, nachdem die nächste Antwortnachricht empfangen worden ist und nachdem die zusätzlichen Daten aus der nächsten Antwortnachricht extrahiert worden sind, die zusätzlichen Daten entschlüsselt, um die Zustandsdaten zu erhalten. Die verschlüsselten Zustandsdaten werden eingesetzt, um das Programm fortzusetzen. Wiederum kann die Anzahl, wie oft die Einmal-Funktion auf die gespeicherte Zufallszahl angewandt wird, um bei einem für den Verschlüsselungsprozess anzuwendenden Schlüssel anzulangen, um 1 reduziert werden für jeden nächsten zu übermittelnden Zustand. Der verwendete Schlüssel in jedem Übermittlungsschritt kann in einem nicht-flüchtigen Teil des Speichers gespeichert werden, es ist jedoch nicht erforderlich, den Schlüssel zu speichern, da er abgeleitet werden kann aus der gespeicherten Zufallszahl und der verwendeten Einmal-Funktion, und, vorzugsweise, aus dem derzeitigen Wert von n, welcher den derzeitigen Zustand identifiziert und welcher möglicherweise in den zusätzlichen Daten enthalten ist.

[0101] Die Schlüssel, welche auf eine Weise erzeugt worden sind, wie sie unter Bezugnahme auf Fig. 4 erläutert wurde, können auch eingesetzt werden in einem Verfahren, in welchem sowohl ein Hash als auch eine Verschlüsselung eingesetzt werden.

[0102] In den angehängten Ansprüchen wird der Begriff „Beziehung" eingesetzt, um anzudeuten, dass zusätzliche Daten sich auf interne Zustandsdaten beziehen. Wie oben erläutert, deutet der Begriff „Beziehung" an, dass die zusätzlichen Daten abgeleitet werden aus den internen Zustandsdaten. Die Beziehung kann zum Beispiel basieren auf einer Gleichheit, oder auf einer Verwendung einer Verschlüsselungstechnologie, kryptographischen Hash-Funktionen und Verschlüsselung mit einem Einmal-Pad.

Patentansprüche

1. Verfahren zur Kommunikation zwischen mindestens einem ersten Gerät (**2**) und einem zweiten Gerät (**10**; **26**);
wobei das erste Gerät (**2**) einen ersten Prozessor (**6**), erste Speichermittel (**4**) und erste Eingabe/Ausgabe-Mittel (**8**) umfasst, wobei die ersten Speichermittel (**4**) und die ersten Eingabe/Ausgabe-Mittel (**8**) mit dem ersten Prozessor (**6**) verbunden sind;
wobei das zweite Gerät (**10**; **26**) einen zweiten Prozessor (**16**; **30**), zweite Speichermittel (**18**; **32**) und zweite Eingabe/Ausgabe-Mittel (**14**; **28**) umfasst, wobei die zweiten Speichermittel (**18**; **32**) und die zweiten Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem zweiten Prozessor (**16**; **30**) verbunden sind;
wobei das Verfahren mindestens die folgenden Schritte umfasst, die von dem ersten Prozessor (**6**) ausgeführt werden:
a. Ausführen eines ersten Programmschritts in Übereinstimmung mit einem vorgegebenen ersten Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nach Ausführung des ersten Programmschritts, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten einschließen, die für das erste Programm erforderlich sind, um fortzufahren, wenn Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;

c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten einschließt, die eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
gefolgt von den folgenden Schritten mittels des zweiten Prozessors (**16**; **30**):
d. Empfangen des ersten Kommunikationsprimitivs;
e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln (**18**; **32**);
f. Ausführen eines zweiten Programmschritts in Übereinstimmung mit einem zweiten Programm;
g. Lesen der ersten zusätzlichen Daten von dem zweiten Speicher;
h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät (**2**), in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten einschließt, die eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen;
gefolgt von den folgenden Schritten, die von dem ersten Prozessor (**6**) ausgeführt werden:
i. Empfangen des zweiten Kommunikationsprimitivs;
j. Extrahieren der zweiten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
l. Ausführen eines dritten Programmschritts in Übereinstimmung mit dem ersten Programm.

2. Verfahren gemäß Anspruch 1, umfassend die folgenden Schritte nach Schritt l:
m. Erstellen von zweiten Zustandsdaten, die sich auf das erste Programm beziehen, nachdem der dritte Programmschritt ausgeführt wurde;
n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät (**10**; **26**), in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv dritte zusätzliche Daten umfasst, welche eine dritte vorgegebene Beziehung zu sowohl den ersten als auch den zweiten Zustandsdaten aufweisen.

3. Verfahren zur Kommunikation zwischen mindestens einem ersten Gerät (**2**) und einem zweiten Gerät (**10**; **26**);
wobei das erste Gerät (**2**) einen ersten Prozessor (**6**), erste Speichermittel (**4**) und erste Eingabe/Ausgabe-Mittel (**8**) umfasst, wobei die ersten Speichermittel (**4**) und die ersten Eingabe/Ausgabe-Mittel (**8**) mit dem ersten Prozessor (**6**) verbunden sind;
wobei das zweite Gerät (**10**; **26**) einen zweiten Prozessor (**16**; **30**), zweite Speichermittel (**18**; **32**) und zweite Eingabe/Ausgabe-Mittel (**14**; **28**) umfasst, wobei die zweiten Speichermittel (**18**; **32**) und die zweiten Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem zweiten Prozessor (**16**; **30**) verbunden sind;
wobei das Verfahren mindestens die folgenden Schritte umfasst, welche von dem ersten Prozessor (**6**) ausgeführt werden:
a. Ausführen eines ersten Programmschritts in Übereinstimmung mit einem vorgegebenen ersten Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der erste Programmschritt ausgeführt wurde, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
gefolgt von den folgenden Schritten mittels des zweiten Prozessors (**16**; **30**):
d. Empfangen des ersten Kommunikationsprimitivs;
e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln (**18**; **32**);
f. Ausführen eines zweiten Programmschritts in Übereinstimmung mit einem zweiten Programm und Erstellen von zweiten Zustandsdaten, welche sich auf das zweite Programm beziehen, nachdem der zweite Programmschritt ausgeführt wurde;
g. Lesen der ersten zusätzlichen Daten aus dem zweiten Speicher;
h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät (**2**), in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten umfasst, welche eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen und dritte zusätzliche Daten, welche eine dritte vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen;
gefolgt von den folgenden Schritten, welche von dem ersten Prozessor (**6**) ausgeführt werden:
i. Empfangen des zweiten Kommunikationsprimitivs;
j. Extrahieren der zweiten und dritten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv, Speichern der dritten zusätzlichen Daten in den ersten Speichermitteln (**4**) und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses;

falls dies der Fall ist, Fortfahren mit:
l. Ausführen eines dritten Programmschritts, in Übereinstimmung mit dem ersten Programm, und Erstellung von dritten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der dritte Programmschritt ausgeführt wurde;
m. Lesen der dritten zusätzlichen Daten aus den ersten Speichermitteln (**4**);
n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät (**10**; **26**), in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv vierte zusätzliche Daten einschließt, welche eine vierte vorgegebene Beziehung zu den dritten zusätzlichen Daten aufweisen und fünfte zusätzliche Daten, welche eine fünfte vorgegebene Beziehung zu den dritten Zustandsdaten aufweisen;
gefolgt von den folgenden Schritten, welche von dem zweiten Prozessor (**16**; **30**) ausgeführt werden:
o. Empfangen des dritten Kommunikationsprimitivs;
p. Extrahieren der vierten und fünften zusätzlichen Daten aus dem dritten Kommunikationsprimitiv; Speichern der fünften zusätzlichen Daten in den zweiten Speichermitteln (**18**; **32**) und Ableiten der dritten zusätzlichen Daten aus den vierten zusätzlichen Daten;
q. Überprüfen, ob die abgeleiteten dritten zusätzlichen Daten die dritte vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des zweiten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
r. Ausführen eines vierten Programmschritts in Übereinstimmung mit dem zweiten Programm.

4. Verfahren gemäß Anspruch 3, wobei Schritt n die folgenden Merkmale aufweist:
n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät (**10**; **26**), in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv die vierten zusätzlichen Daten aufweist und fünfte zusätzliche Daten, welche eine fünfte vorgegebene Beziehung zu sowohl den ersten als auch den dritten Zustandsdaten aufweisen.

5. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei der Schritt c die folgenden Teilschritte umfasst:
c1. Übermitteln eines ersten Kommunikationsprimitivs, welches zusätzliche Daten umfasst, die eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen, in Übereinstimmung mit dem ersten Programm, an einen zentralen Speicher (**34**);
c2. Speichern des ersten Kommunikationsprimitivs in dem zentralen Speicher (**34**);
und wobei Schritt d die folgenden Teilschritte umfasst:
d1. Überprüfen, ob der zentrale Speicher (**34**) das erste Kommunikationsprimitiv gespeichert hat; falls dies nicht der Fall ist, Wiederholen von Schritt d1; falls dies der Fall ist, Fortfahren mit Schritt d2;
d2. Lesen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**);
d3. Entfernen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**).

6. Verfahren gemäß einem der Ansprüche 1 bis 4, wobei der Schritt c die folgenden Teilschritte umfasst:
c1. Übermitteln eines ersten Kommunikationsprimitivs, welches zusätzliche Daten umfasst, die eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen, in Übereinstimmung mit dem ersten Programm, an einen zentralen Speicher (**34**);
c2. Speichern des ersten Kommunikationsprimitivs in dem zentralen Speicher (**34**); und wobei Schritt d die folgenden Teilschritte umfasst:
d1. Überprüfen, ob der zentrale Speicher (**34**) das erste Kommunikationsprimitiv gespeichert hat; falls dies nicht der Fall ist, Wiederholen von Schritt d1; falls dies der Fall ist, Fortfahren mit Schritt d2;
d2. Lesen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**);
d3. Hinzufügen eines Hinweises zu dem ersten Kommunikationsprimitiv in dem zentralen Speicher (**34**), dass das erste Kommunikationsprimitiv von dem zweiten Gerät (**10**; **26**) gelesen worden ist.

7. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei mindestens das erste und das zweite Kommunikationsprimitiv Identifikationsdaten umfassen, um zu identifizieren, dass das erste und das zweite Kommunikationsprimitiv die ersten zusätzlichen Daten umfassen.

8. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die erste Beziehung basiert auf einer Verwendung von einer oder mehrerer der folgenden Verfahren, entweder einzeln oder in Kombination: Anwenden eines ersten Verschlüsselungsverfahrens, Anwenden einer ersten kryptographischen Hashfunktion, und Anwenden einer zweiten Verschlüsselung mit Einmal-Pad-Funktion.

9. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die erste Beziehung basiert auf einer Verwendung einer oder mehrerer der folgenden Verfahren, entweder allein oder in Kombination: Anwenden eines zweiten Verschlüsselungsverfahrens, Anwenden einer zweiten kryptographischen Hashfunktion, und Anwenden einer zweiten Verschlüsselung mit Einmal-Pad-Funktion.

10. System, umfassend mindestens ein erstes Gerät (**2**) und ein zweites Gerät (**10**; **26**);
wobei das erste Gerät (**2**) einen ersten Prozessor (**6**), erste Speichermittel (**4**) und erste Eingabe/Ausgabe-Mittel (**8**) umfasst, wobei die ersten Speichermittel (**4**) und die ersten Eingabe/Ausgabe-Mittel (**8**) mit dem ersten Prozessor (**6**) verbunden sind;
wobei das zweite Gerät (**10**; **26**) einen zweiten Prozessor (**16**; **30**), zweite Speichermittel (**18**; **32**) und

zweite Eingabe/Ausgabe-Mittel (**14**; **28**) umfasst, wobei die zweiten Speichermittel (**18**; **32**) und die zweiten Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem zweiten Prozessor (**16**; **30**) verbunden sind;
wobei der erste Prozessor (**6**) eingerichtet ist, um mindestens die folgenden Schritte auszuführen:
a. Ausführen eines ersten Programmschritts in Übereinstimmung mit einem vorgegebenen ersten Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der erste Programmschritt ausgeführt wurde, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
wobei der zweite Prozessor (**16**; **30**) eingerichtet ist, um die folgenden Schritte auszuführen, nachdem der erste Prozessor (**6**) die Schritte a bis c ausgeführt hat:
d. Empfangen des ersten Kommunikationsprimitivs;
e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln (**18**, **32**);
f. Ausführen eines zweiten Programmschritts, in Übereinstimmung mit einem zweiten Programm;
g. Lesen der ersten zusätzlichen Daten aus dem zweiten Speicher;
h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät (**2**), in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten umfasst, die eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen;
wobei der erste Prozessor (**6**) auch eingerichtet ist, um die folgenden Schritte auszuführen, nachdem der zweite Prozessor (**16**; **30**) die Schritte d bis h ausgeführt hat:
i. Empfangen des zweiten Kommunikationsprimitivs;
j. Extrahieren der zweiten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
l. Ausführen eines dritten Programmschritts, in Übereinstimmung mit dem ersten Programm.

11. System, umfassend mindestens ein erstes Gerät (**2**) und ein zweites Gerät (**10**; **26**);
wobei das erste Gerät (**2**) einen ersten Prozessor (**6**), erste Speichermittel (**4**) und erste Eingabe/Ausgabe-Mittel (**8**) umfasst, wobei die ersten Speichermittel (**4**) und die ersten Eingabe/Ausgabe-Mittel (**8**) mit dem ersten Prozessor (**6**) verbunden sind;
wobei das zweite Gerät (**10**; **26**) einen zweiten Prozessor (**16**; **30**), zweite Speichermittel (**18**; **32**) und zweite Eingabe/Ausgabe-Mittel (**14**; **28**), umfasst, wobei die zweiten Speichermittel (**18**; **32**) und die zweiten Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem zweiten Prozessor (**16**; **30**) verbunden sind;
wobei der erste Prozessor (**6**) eingerichtet ist, um mindestens die folgenden Schritte auszuführen:
a. Ausführen eines ersten Programmschritts, in Übereinstimmung mit einem vorgegebenen ersten Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der erste Programmschritt ausgeführt wurde, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten einschließt, die eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
wobei der zweite Prozessor (**16**; **30**) eingerichtet ist, um die folgenden Schritte auszuführen, nachdem der erste Prozessor (**6**) die Schritte a bis c ausgeführt hat:
d. Empfangen des ersten Kommunikationsprimitivs;
e. Extrahieren der ersten zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der ersten zusätzlichen Daten in den zweiten Speichermitteln (**18**; **32**);
f. Ausführen eines zweiten Programmschritts, in Übereinstimmung mit einem zweiten Programm und Erstellen von zweiten Zustandsdaten, welche sich auf das zweite Programm beziehen, nachdem der zweite Programmschritt ausgeführt worden ist;
g. Lesen der ersten zusätzlichen Daten aus dem zweiten Speicher;
h. Übermitteln eines zweiten Kommunikationsprimitivs an das erste Gerät (**2**), in Übereinstimmung mit dem zweiten Programm, wobei das erste Kommunikationsprimitiv zweite zusätzliche Daten umfasst, die eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen, und dritte zusätzliche Daten, welche eine dritte vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen;
wobei der erste Prozessor (**6**) weiterhin eingerichtet ist, um die folgenden Schritte auszuführen, nachdem der zweite Prozessor (**16**; **30**) die Schritte d bis h ausgeführt hat.
i. Empfangen des zweiten Kommunikationsprimitivs;
j. Extrahieren der zweiten und dritten zusätzlichen

Daten aus dem zweiten Kommunikationsprimitiv, Speichern der dritten zusätzlichen Daten in den ersten Speichermitteln (**4**) und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
k. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten eine erste vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des ersten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
l. Ausführen eines dritten Programmschritts, in Übereinstimmung mit dem ersten Programm, und Erstellen von dritten Zustandsdaten, welche sich auf das erste Programm beziehen, nachdem der dritte Programmschritt ausgeführt worden ist;
m. Lesen der dritten zusätzlichen Daten aus den ersten Speichermitteln (**4**);
n. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät (**10**; **26**), in Übereinstimmung mit dem ersten Programm, wobei das dritte Kommunikationsprimitiv vierte zusätzliche Daten umfasst, die eine vierte vorgegebene Beziehung zu den dritten zusätzlichen Daten aufweisen, und fünfte zusätzliche Daten, welche eine fünfte vorgegebene Beziehung zu den dritten Zustandsdaten aufweisen;
wobei der zweite Prozessor (**16**; **30**) weiterhin eingerichtet ist, um die folgenden Schritte auszuführen, nachdem der erste Prozessor (**6**) die Schritte i bis n ausgeführt hat:
o. Empfangen des dritten Kommunikationsprimitivs;
p. Extrahieren der vierten und fünften zusätzlichen Daten aus dem dritten Kommunikationsprimitiv, Speichern der fünften zusätzlichen Daten in den zweiten Speichermitteln (**18**; **32**) und Ableiten der dritten zusätzlichen Daten aus den vierten zusätzlichen Daten;
q. Überprüfen, ob die abgeleiteten dritten zusätzlichen Daten eine dritte vorgegebene Beziehung zu den zweiten Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des zweiten Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
r. Ausführen eines vierten Programmschritts, in Übereinstimmung mit dem zweiten Programm.

12. Gerät, umfassend einen Prozessor (**6**), Speichermittel (**4**) und Eingabe/Ausgabe-Mittel (**8**), wobei die Speichermittel (**4**) und die Eingabe/Ausgabe-Mittel (**8**) mit dem Prozessor (**6**) verbunden sind;
wobei der Prozessor (**6**) eingerichtet ist, um mindestens die folgenden Schritte auszuführen:
a. Ausführen eines ersten Programmschritts, in Übereinstimmung mit einem vorgegebenen Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das Programm beziehen, nachdem der erste Programmschritt ausgeführt worden ist, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten umfassen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem ersten Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
d. Empfangen eines zweiten Kommunikationsprimitivs von einem anderen Gerät;
e. Extrahieren von zweiten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
f. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten die vorgegebene Beziehung zu den Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
g. Ausführen eines zweiten Programmschritts, in Übereinstimmung mit dem Programm.

13. Gerät gemäß Anspruch 12, wobei der Prozessor (**6**) eingerichtet ist, um nach Schritt g die folgenden Schritte auszuführen:
h. Erstellen von zweiten Zustandsdaten, welche sich auf das Programm beziehen, nachdem der zweite Programmschritt ausgeführt worden ist;
i. Übermitteln eines dritten Kommunikationsprimitivs an das zweite Gerät (**10**; **26**), in Übereinstimmung mit dem Programm, wobei das dritte Kommunikationsprimitiv dritte zusätzliche Daten umfasst, welche eine dritte vorgegebene Beziehung zu sowohl den ersten als auch den zweiten Zustandsdaten aufweisen.

14. Gerät gemäß Anspruch 12 oder 13, wobei das Gerät eine Smart Card ist.

15. Gerät gemäß einem der Ansprüche 12 bis 14, wobei der Prozessor (**6**) eingerichtet ist, um nach einer Unterbrechung und Wiederherstellung der Energieversorgung des Prozessors (**6**) die folgenden Schritte auszuführen:
Empfangen mindestens eines Kommunikationsprimitivs von entweder dem anderen Gerät oder einem zentralen Speicher (**34**), wobei das Kommunikationsprimitiv eine vorgegebene Beziehung zu letzten Zustandsdaten aufweist, die in Übereinstimmung mit einem letzten Programmschritt erstellt wurden, der von dem ersten Programm ausgeführt worden ist;
Wiederaufnehmen der Ausführung des ersten Programms mit einem weiteren Programmschritt, welcher auf diesen letzten Programmschritt folgt.

16. Computerprogrammprodukt, umfassend Computer-ausführbare Instruktionen zur Ausführung durch eine Computervorrichtung, die einen Prozessor (**6**), Speichermittel (**4**) und Eingabe/Ausgabe-Mittel (**8**) umfasst, wobei die Speichermittel (**4**) und die Eingabe/Ausgabe-Mittel (**8**) mit dem Prozessor (**6**) verbunden sind, wobei das Computerprogrammpro-

dukt es dem Prozessor (**6**) ermöglicht, mindestens die folgenden Schritte auszuführen:
a. Ausführen eines ersten Programmschritts, in Übereinstimmung mit dem Programm;
b. Erstellen von ersten Zustandsdaten, welche sich auf das Programm beziehen, nachdem der erste Programmschritt ausgeführt worden ist, wobei die ersten Zustandsdaten in den ersten Speichermitteln (**4**) gespeichert sind und alle Daten einschließen, welche für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem zweiten Prozessor (**16**; **30**) empfangen worden sind;
c. Übermitteln eines ersten Kommunikationsprimitivs, in Übereinstimmung mit dem Programm, wobei das erste Kommunikationsprimitiv erste zusätzliche Daten umfasst, welche eine vorgegebene Beziehung zu den ersten Zustandsdaten aufweisen;
d. Empfangen eines zweiten Kommunikationsprimitivs von einem anderen Gerät;
e. Extrahieren der zweiten zusätzlichen Daten aus dem zweiten Kommunikationsprimitiv und Ableiten der ersten zusätzlichen Daten aus den zweiten zusätzlichen Daten;
f. Überprüfen, ob die abgeleiteten ersten zusätzlichen Daten eine vorgegebene Beziehung zu den Zustandsdaten aufweisen; falls dies nicht der Fall ist, entweder Abbrechen des Programms oder Starten eines Wiederherstellungsprozesses; falls dies der Fall ist, Fortfahren mit:
g. Ausführen eines zweiten Programmschritts, in Übereinstimmung mit dem Programm.

17. Computer-lesbares Medium, ausgestattet mit einem Computerprogrammprodukt gemäß Anspruch 16.

18. Gerät (**10**; **26**), umfassend einen Prozessor (**16**; **30**), Speichermittel (**18**; **32**) und Eingabe/Ausgabe-Mittel (**14**; **28**) wobei die Speichermittel (**18**; **32**) und die Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem Prozessor (**16**; **30**) verbunden sind;
wobei der Prozessor (**16**; **30**) eingerichtet ist, um die folgenden Schritte auszuführen:
a. Empfangen eines ersten Kommunikationsprimitivs von einem anderen Gerät (**2**);
b. Erkennen, dass das erste Kommunikationsprimitiv zusätzliche Daten umfasst, welche eine erste vorgegebene Beziehung zu Zustandsdaten aufweisen, die sich auf ein erstes Programm beziehen, welches auf dem anderen Gerät (**2**) abläuft, wobei die Zustandsdaten alle Daten umfassen, die für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem Prozessor (**16**; **30**) empfangen worden sind;
c. Extrahieren der zusätzlichen Daten aus dem ersten Kommunikationsprimitiv und Speichern der zusätzlichen Daten in den Speichermitteln (**18**; **32**);
d. Ausführen eines Programmschritts, in Übereinstimmung mit einem zweiten Programm;
e. Lesen der ersten zusätzlichen Daten aus dem Speicher;
f. Übermitteln eines zweiten Kommunikationsprimitivs an das andere Gerät (**2**), in Übereinstimmung mit dem zweiten Programm, wobei das zweite Kommunikationsprimitiv zweite zusätzliche Daten umfasst, welche eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen.

19. Gerät gemäß Anspruch 18, wobei das Gerät ein Terminal ist, welches eingerichtet ist, mit einer Smart Card zu kommunizieren.

20. Gerät gemäß Anspruch 18 oder 19, wobei der Prozessor (**16**; **30**) eingerichtet ist, um die folgenden Teilschritte in Schritt a auszuführen:
a1. Überprüfen, ob ein zentraler Speicher (**34**) das erste Kommunikationsprimitiv gespeichert hat; falls dies nicht der Fall ist, Wiederholen von Schritt a1; falls dies der Fall ist, Fortfahren mit Schritt a2;
a2. Lesen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**);
a3. Entfernen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**).

21. Gerät gemäß Anspruch 18 oder 19, wobei der Prozessor (**16**; **30**) eingerichtet ist, um die folgenden Teilschritte in Schritt a auszuführen.
a1. Überprüfen, ob ein zentraler Speicher (**34**) das erste Kommunikationsprimitiv gespeichert hat; falls dies nicht der Fall ist, Wiederholen von Schritt a1; falls dies der Fall ist, Fortfahren mit Schritt a2;
a2. Lesen des ersten Kommunikationsprimitivs aus dem zentralen Speicher (**34**);
a3. Hinzufügen eines Hinweises zu dem ersten Kommunikationsprimitiv in dem zentralen Speicher (**34**), dass das erste Kommunikationsprimitiv von dem Gerät (**10**; **26**) gelesen worden ist.

22. Computerprogrammprodukt, umfassend Computer-ausführbare Instruktionen zur Ausführung durch eine Computervorrichtung (**10**; **26**), die einen Prozessor (**16**; **30**), Speichermittel (**18**; **32**) und Eingabe/Ausgabe-Mittel (**14**; **28**) umfasst, wobei die Speichermittel (**18**; **32**) und die Eingabe/Ausgabe-Mittel (**14**; **28**) mit dem Prozessor (**16**; **30**) verbunden sind, wobei das Computerprogrammprodukt es dem Prozessor (**6**) ermöglicht, mindestens die folgenden Schritte auszuführen:
a. Empfangen eines ersten Kommunikationsprimitivs von einem anderen Gerät (**2**);
b. Erkennen, dass das erste Kommunikationsprimitiv zusätzliche Daten umfasst, die eine vorgegebene erste Beziehung zu Zustandsdaten aufweisen, die sich auf ein erstes Programm beziehen, welches auf dem anderen Gerät (**2**) abläuft, wobei die Zustandsdaten alle Daten umfassen, die für das erste Programm erforderlich sind, um fortzufahren, nachdem Instruktionen von dem Prozessor (**16**; **30**) empfangen worden sind;
c. Extrahieren der zusätzlichen Daten aus dem ers-

ten Kommunikationsprimitiv und Speichern der zusätzlichen Daten in den Speichermitteln (**18**; **32**);
d. Ausführen eines ersten Programmschritts, in Übereinstimmung mit dem Programm;
e. Lesen der ersten zusätzlichen Daten aus dem Speicher;
f. Übermitteln eines zweiten Kommunikationsprimitivs an das andere Gerät (**2**), in Übereinstimmung mit dem Programm, wobei das zweite Kommunikationsprimitiv die zweiten zusätzlichen Daten umfasst, die eine zweite vorgegebene Beziehung zu den ersten zusätzlichen Daten aufweisen.

23. Computer-lesbares Medium, welches ausgestattet ist mit einem Computerprogrammprodukt gemäß Anspruch 22.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

Fig 1 Stand der Technik

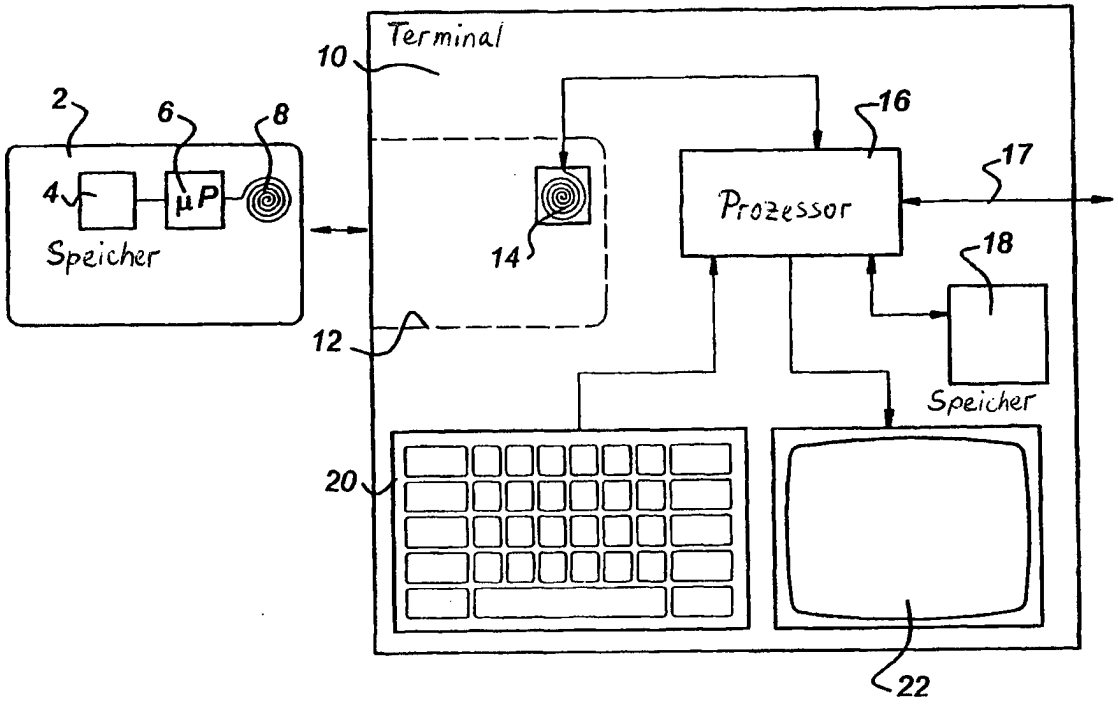


Fig 2

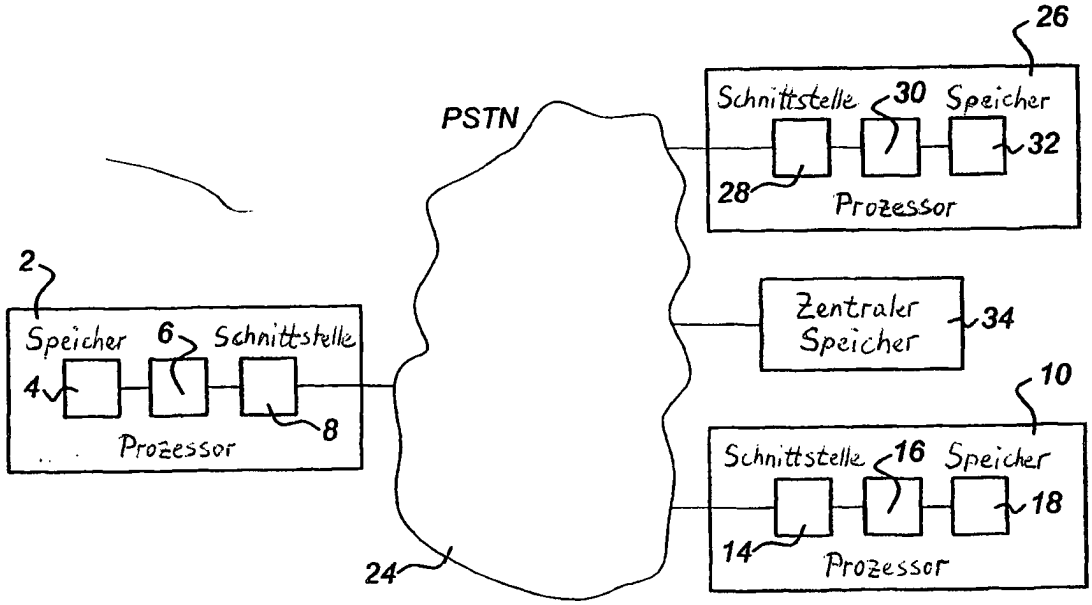


Fig 3a

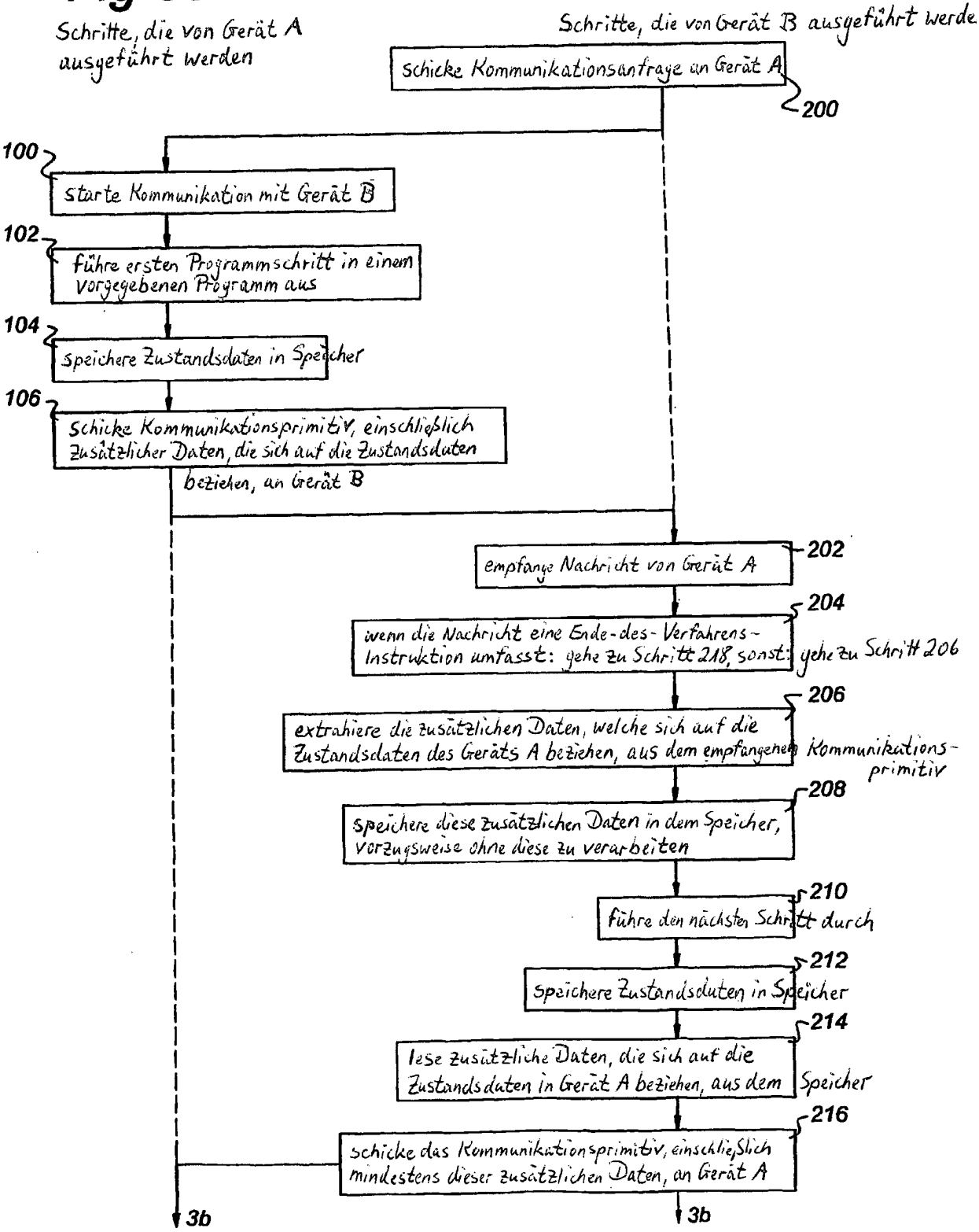

Schritte, die von Gerät A ausgeführt werden
Schritte, die von Gerät B ausgeführt werde
schicke Kommunikationsanfrage an Gerät A
200
100
starte Kommunikation mit Gerät B
102
führe ersten Programmschritt in einem vorgegebenen Programm aus
104
speichere Zustandsdaten in Speicher
106
schicke Kommunikationsprimitiv, einschließlich zusätzlicher Daten, die sich auf die Zustandsdaten beziehen, an Gerät B
empfange Nachricht von Gerät A
202
204
wenn die Nachricht eine Ende-des-Verfahrens-Instruktion umfasst: gehe zu Schritt 218, sonst: gehe zu Schritt 206
206
extrahiere die zusätzlichen Daten, welche sich auf die Zustandsdaten des Geräts A beziehen, aus dem empfangenen Kommunikations-primitiv
208
speichere diese zusätzlichen Daten in dem Speicher, vorzugsweise ohne diese zu verarbeiten
210
führe den nächsten Schritt durch
212
speichere Zustandsdaten in Speicher
214
lese zusätzliche Daten, die sich auf die Zustandsdaten in Gerät A beziehen, aus dem Speicher
216
schicke das Kommunikationsprimitiv, einschließlich mindestens dieser zusätzlichen Daten, an Gerät A
3b
3b

Fig 3b

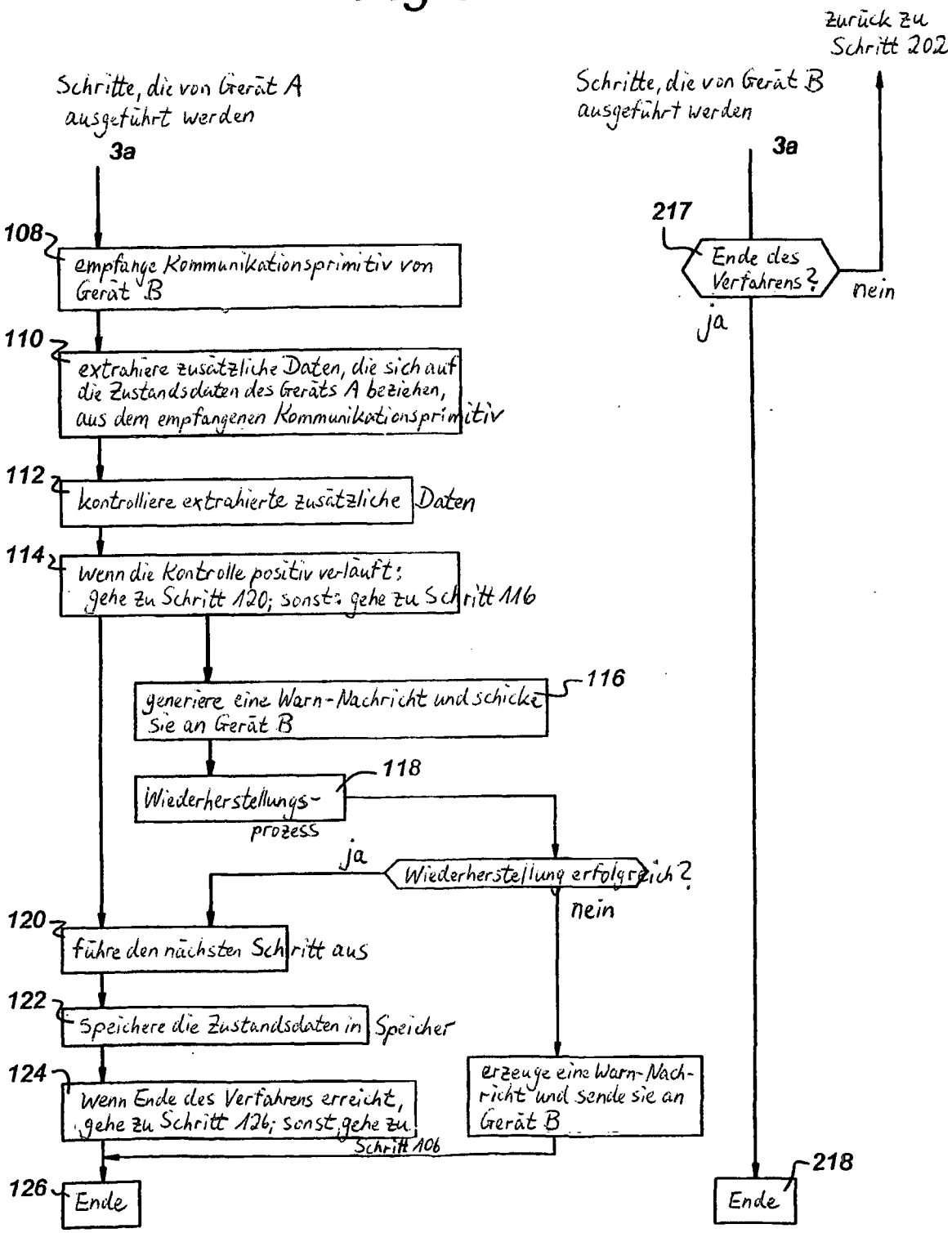
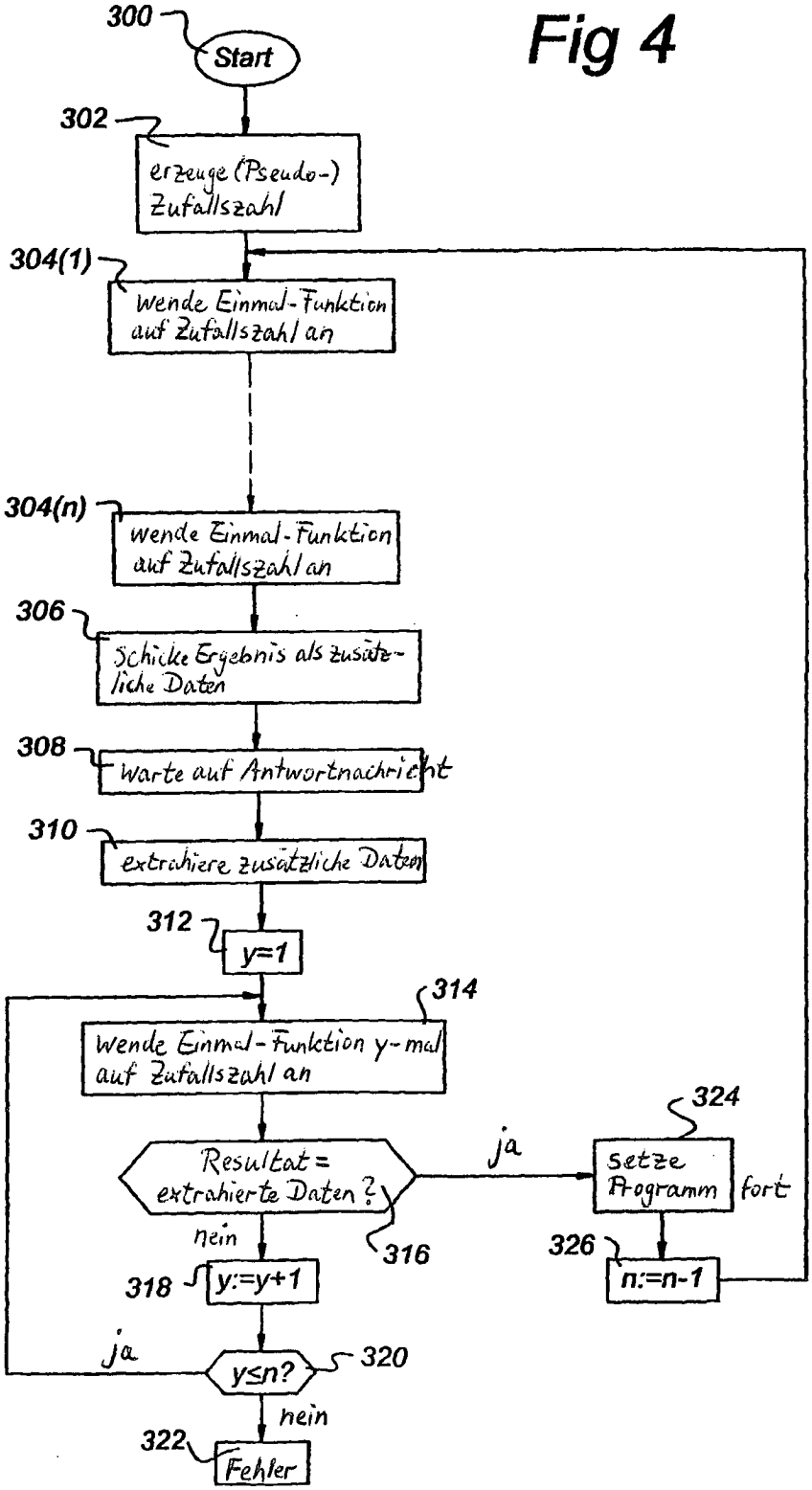

Schritte, die von Gerät A ausgeführt werden
3a
108
empfange Kommunikationsprimitiv von Gerät B
110
extrahiere zusätzliche Daten, die sich auf die Zustandsdaten des Geräts A beziehen, aus dem empfangenen Kommunikationsprimitiv
112
kontrolliere extrahierte zusätzliche Daten
114
Wenn die Kontrolle positiv verläuft: gehe zu Schritt 120; sonst: gehe zu Schritt 116
116
generiere eine Warn-Nachricht und schicke sie an Gerät B
118
Wiederherstellungs-prozess
ja
Wiederherstellung erfolgreich?
nein
120
führe den nächsten Schritt aus
122
Speichere die Zustandsdaten in Speicher
124
Wenn Ende des Verfahrens erreicht, gehe zu Schritt 126; sonst gehe zu Schritt 106
126
Ende
erzeuge eine Warn-Nachricht und sende sie an Gerät B
Schritte, die von Gerät B ausgeführt werden
Zurück zu Schritt 202
3a
217
Ende des Verfahrens?
nein
ja
218
Ende

Fig 4


300
Start
302
erzeuge (Pseudo-) Zufallszahl
304(1)
wende Einmal-Funktion auf Zufallszahl an
304(n)
wende Einmal-Funktion auf Zufallszahl an
306
Schicke Ergebnis als zusätzliche Daten
308
Warte auf Antwortnachricht
310
extrahiere zusätzliche Daten
312
y=1
314
wende Einmal-Funktion y-mal auf Zufallszahl an
Resultat = extrahierte Daten?
ja
nein
316
324
setze Programm fort
326
n:=n-1
318
y:=y+1
ja
y≤n?
320
nein
322
Fehler