(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 603 07 498 T2** 2007.09.13

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 559 256 B1**
(21) Deutsches Aktenzeichen: **603 07 498.7**
(86) PCT-Aktenzeichen: **PCT/IB03/04720**
(96) Europäisches Aktenzeichen: **03 751 197.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2004/043037**
(86) PCT-Anmeldetag: **24.10.2003**
(87) Veröffentlichungstag der PCT-Anmeldung: **21.05.2004**
(97) Erstveröffentlichung durch das EPA: **03.08.2005**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.08.2006**
(47) Veröffentlichungstag im Patentblatt: **13.09.2007**

(51) Int Cl.[8]: ***H04L 29/06*** (2006.01)

(30) Unionspriorität:
02405954 06.11.2002 EP

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(73) Patentinhaber:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Duscher, R., Dipl.-Phys. Dr.rer.nat., Pat.-Ass., 71034 Böblingen

(72) Erfinder:
BAENTSCH, Michael, CH-8135 Langnau, CH; BUHLER, Peter, CH-8810 Horgen, CH; EIRICH, Thomas, CH-8820 Waedenswil, CH; HÖRING, Frank, ch-8006 Zurich, CH; KRAMP, Thorsten, CH-8802 Kilchberg, CH; OESTREICHER, Marcus, CH-8003 Zurich, CH; OSBORNE, Michael, CH-8804 Au, CH; WEIGOLD, D., Thomas, CH-8800 Thalwil, CH

(54) Bezeichnung: **BEREITSTELLEN EINES BENUTZERGERÄTES MIT EINER ZUGANGSKODESAMMLUNG**

Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Erfindung betrifft allgemein Verfahren, Einrichtungen und Computerprogrammelemente zum Bereitstellen eines Benutzergerätes mit einem Satz Zugangscodes, wie beispielsweise Einmal-Authentifizierungscodes, über Datenübertragungsnetze, wie zum Beispiel drahtlose Datenübertragungsnetze.

[0002] Bei Online-Transaktionen erfreuen sich Einmal-Authentifizierungscodes (One Time Authentication Code, OTAC) mit gedruckten Abstreichlisten von Transaktions-Authentifizierungsnummern (Transaction Authentication Number, TAN) oder Einmal-Kreditkartennummern zunehmender Beliebtheit. Es wäre wünschenswert, eine sichere Speicherung und Verteilung von OTACs zu ermöglichen. Desgleichen wäre es wünschenswert, immer und überall bei Bedarf bequem auf die OTACs zugreifen zu können. Gedruckte Abstreichlisten sind jedoch leider relativ unsicher und nicht immer einfach verfügbar. Normalerweise wird eine Abstreichliste von einem Dienstanbieter, wie beispielsweise einer Bank, mit normaler Post an einen Kunden gesendet. Eine Abstreichliste kann auf dem Postweg zum Kunden abgefangen und kopiert werden. Außerdem ist bei vielen Kunden nicht damit zu rechnen, dass sie die Abstreichlisten an einem sicheren Ort, wie beispielsweise in einem Safe, aufbewahren. Das ist insbesondere dann der Fall, wenn die Abstreichliste regelmäßig benutzt wird. Eine regelmäßig benutzte Abstreichliste kann möglicherweise offen liegen bleiben, zum Beispiel auf einem Schreibtisch. Dadurch erlangen andere Personen Zugang zu der Abstreichliste. Wenn ein Kunde die Abstreichliste mit sich führt, kann sie verloren gehen oder gestohlen werden. OTACs in Abstreichlisten sind normalerweise nicht verschlüsselt. Die Kontonummern von Kunden, welche zum Ausführen einer Transaktion im Allgemeinen mit einem OTAC kombiniert werden, gelten praktisch als offen bekannt. Viele Kunden empfinden es als unbequem, die bereits benutzten OTACs manuell zu verwalten. Beim Wechsel von einer zur nächsten Abstreichliste müssen Kunden zeitweilig zwei Abstreichlisten aufbewahren oder bei sich haben. Dadurch erhöht sich das Sicherheitsrisiko. Außerdem stellt es für den ausgebenden Dienstanbieter eine komplizierte Aufgabe dar, die Abstreichlisten zu drucken und rechtzeitig zu versenden.

[0003] In der US-Patentschrift 2002/141588 wird ein Mechanismus für einen Benutzer, der eine zu übertragende Datei anfordert, und für einen Server beschrieben, der die angeforderte Datei verschlüsselt und dem anfordernden Benutzer zustellt.

[0004] In der Patentschrift WO98/37524 wird ein Transaktionsverfahren beschrieben, das eine mobile Einrichtung verwendet. Dieses Verfahren bedient sich der Kennzeichnung von Einzelkonten der internationalen Abbuchungsbenutzerkennnummern (International Debit User Identification, IDUI). Die IDUI entspricht einer normalen Kontonummer eines Bankkunden. Die IDUI wird vorher auf eine Kredit-/Geldkarte geladen. Während der Benutzung liest ein Kassenterminal (Point Of Sale, POS) die IDUI von einer Kredit-/Geldkarte und zeigt einen von einem angegebenen Konto abzubuchenden Betrag an. Der Kunde schließt die Transaktion durch Drücken einer Bestätigungstaste am Kassenterminal ab. Das Kassenterminal sendet eine Transaktionsquittung an einen Server in der für das Konto zuständigen Bank. In der Patentschrift WO98/37524 wird vorgeschlagen, die IDUI vorher nicht auf einem Magnetstreifen oder einer Speicherkarte zu speichern, sondern auf einer Smartcard mit Kundenkennungsmodul (Subscriber Identification Module, SIM), wie sie bei GSM-Mobilfunknetzen verwendet wird. Die IDUI wird dann durch das Terminal berührungslos von der Smartcard gelesen. Zur Prüfung werden dann Transaktionsquittungen mittels SMS-Nachrichten zum Server gesendet. Bei dieser Verfahrensweise wird nur die Verwendung von IDUIs für Transaktionen mit Kassenterminals über eine berührungslose Schnittstelle und die Übertragung von SMS-Nachrichten zum Prüfen der Transaktion erörtert. Das Verfahren eignet sich aber nicht zum Zustellen von OTAC-Listen. Das liegt daran, dass die IDUIs für jedes Konto unveränderlich sind. Auf OTACs trifft dies jedoch nicht zu. Ähnliche elektronische Zahlungssysteme werden in den Patentschriften EP1 176 844, WO99/16029, WO00/495585, WO01/09851, WO02/21464 und WO01/93528 beschrieben.

[0005] Das Ziel der vorliegenden Erfindung besteht darin, diese Aufgabe mit Hilfe der Verfahren, des Computerprogramms und der Einrichtungen gemäß den Ansprüchen 1, 7, 13, 17, 22, 34 und 38 zu lösen. Vorteilhafte Ausführungsarten davon sind in den entsprechenden Unteransprüchen definiert.

[0006] Gemäß der vorliegenden Erfindung wird ein Verfahren zum Bereitstellen eines Benutzergerätes mit einem Satz Zugangscodes bereitgestellt, wobei das Verfahren Folgendes umfasst: in dem Benutzergerät, Speichern eines kryptografischen Schlüssels und eines Kennungscodes und Senden einer Nachricht, welche den Kennungscode enthält, über ein Datenübertragungsnetz an einen Server; im Server, Speichern eines kryptografischen Schlüssels, der dem in dem Benutzergerät gespeicherten Schlüssel entspricht, Zuweisen des Satzes von Zugangscodes nach dem Empfang des Kennungscodes von dem Benutzergerät, Durchführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels aus dem Speicher, Verschlüsseln des Satzes von Zugangscodes

mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes und Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät; und, in dem Benutzergerät, Entschlüsseln des vom Server empfangenen verschlüsselten Satzes mittels des Schlüssels aus dem Speicher und Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes.

[0007] Dadurch können Kunden bequem und sicher mit Zugangscodes, wie beispielsweise OTACs, versorgt werden.

[0008] Vorzugsweise umfasst das Verfahren außerdem: im Server, Erzeugen eines neuen Schlüssels, Verschlüsseln des neuen Schlüssels mit dem vorherigen Schlüssel und Senden einer Nachricht, welche den verschlüsselten neuen Schlüssel enthält, über das Netz an das Benutzergerät; und, in dem Benutzergerät, Entschlüsseln des vom Server empfangenen neuen Schlüssels mittels des vorherigen Schlüssels und Speichern des entschlüsselten neuen Schlüssels anstelle des vorherigen Schlüssels.

[0009] Dadurch wird die Sicherheit auf vorteilhafte Weise erhöht, indem die sichere Erneuerung von benutzten Schlüsseln erleichtert wird.

[0010] Das Verfahren kann auch ausgedehnt werden auf: im Server, Verschlüsseln eines neuen Satzes von Zugangscodes mit dem neuen Schlüssel zum Erzeugen eines mit dem neuen Schlüssel verschlüsselten Satzes und Senden einer Nachricht, welche den mit dem neuen Schlüssel verschlüsselten Satz enthält, über das Netz an das Benutzergerät; und, in dem Benutzergerät, Entschlüsseln des mit dem neuen Schlüssel verschlüsselten Satzes mittels des neuen Schlüssels und Speichern des entschlüsselten neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

[0011] Dadurch werden die Zugangscodes auf vorteilhafte Weise bequem erneuert.

[0012] Vorzugsweise umfasst das Verfahren ferner: im Server, Senden einer Nachricht, welche einen neuen Satz Zugangscodes enthält, über das Netz an das Benutzergerät; und in dem Benutzergerät, Speichern des neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes. Das Verfahren kann ferner Folgendes umfassen: in dem Benutzergerät, Überwachen der durch den Benutzer benutzten Zugangscodes, Erzeugen einer Anforderung als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes der Anzahl unbenutzter Zugangscodes und Senden einer Nachricht, welche die Anforderung enthält, an den Server; und im Server, Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, nach dem Empfang der Anforderung. Alternativ kann das Verfahren Folgendes umfassen: im Server, Überwachen der durch den Benutzer benutzten Zugangscodes und Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, an das Benutzergerät als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes der Anzahl unbenutzter Zugangscodes. Bei einer anderen Alternative kann das Verfahren Folgendes umfassten: in dem Benutzergerät, Erzeugen einer Anforderung als Reaktion auf eine manuelle Eingabe vom Benutzer und Senden einer Nachricht, welche die Anforderung enthält, an den Server; und im Server, Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, nach dem Empfang der Anforderung.

[0013] Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung umfasst das Verfahren ferner Folgendes: in dem Benutzergerät, Erzeugen eines Paars öffentlicher/privater Schlüssel und Senden einer Nachricht, welche den öffentlichen Schlüssel des Paars enthält, über das Netz an den Server; im Server, Erzeugen eines Sitzungsschlüssels, verschlüsseln des Satzes von Zugangscodes mit dem Sitzungsschlüssel zum Erzeugen eines mit dem Sitzungsschlüssel verschlüsselten Satzes, Verschlüsseln des Sitzungsschlüssels mit dem öffentlichen Schlüssel zum Erzeugen eines verschlüsselten Sitzungsschlüssels, Senden einer Nachricht, welche den mit dem Sitzungsschlüssel verschlüsselten Satz und den verschlüsselten Sitzungsschlüssel enthält, über das Netz an das Benutzergerät; und in dem Benutzergerät, Entschlüsseln des verschlüsselten Sitzungsschlüssels mit dem privaten Schlüssel des Paars zum Wiederherstellen des Sitzungsschlüssels, Entschlüsseln des mit dem Sitzungsschlüssel verschlüsselten Satzes mit dem wiederhergestellten Sitzungsschlüssel zum Wiederherstellen des Satzes und Speichern des entschlüsselten Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

[0014] Dadurch wird die Sicherheit auf vorteilhafte Weise durch die Verschlüsselung mit mehreren Schlüsseln erhöht.

[0015] Unter einem anderen Aspekt der vorliegenden Erfindung wird im Folgenden ein Verfahren zum Versorgen eines Benutzergerätes mit einem Satz von Zugangscodes bereitgestellt, wobei das Verfahren in dem Benutzergerät Folgendes umfasst: Speichern eines kryptografischen Schlüssels und eines Kennungscodes; Senden einer Nachricht, welche den Kennungscodes enthält, über ein Datenübertragungsnetz an einen Server; Empfangen einer Nachricht, welche den Satz der mit dem Schlüssel verschlüsselten Zugangscodes enthält, vom Server; Entschlüsseln des empfangenen Satzes von Zugangscodes mittels des im Speicher gespeicherten Schlüssels; und Speichern des entschlüsselten Sat-

zes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes. Die vorliegende Erfindung erstreckt sich auch auf ein Computerprogrammelement, welches Computerprogrammcodemittel umfasst, die in einen Prozessor eines Benutzergerätes geladen werden und den Prozessor so konfigurieren, dass er ein in diesem Kapitel beschriebenes Verfahren durchführt.

[0016] Unter einem weiteren Aspekt wird im Folgenden ein Verfahren zum Versorgen eines Benutzergerätes mit einem Satz von Zugangscodes bereitgestellt, wobei das Verfahren in einem Server zur Datenübertragung mit dem Benutzergerät über ein Netz Folgendes umfasst: Speichern eines kryptografischen Schlüssels, welcher einem in dem Benutzergerät gespeicherten kryptografischen Schlüssel entspricht; Zuweisen des Satzes von Zugangscodes zu dem Benutzergerät nach dem Empfang einer Nachricht, welche einen Kennungscode enthält, über das Netz von dem Benutzergerät; Ausführen einer Suchfunktion unter Verwendung des in der Nachricht empfangenen Kennungscodes, um den Schlüssel vom Speicher abzurufen; Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes; und Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät. Die vorliegende Erfindung erstreckt sich auch auf ein Computerprogrammelement, welches Computerprogrammcodemittel umfasst, die in einen Prozessor eines Server-Computersystems geladen werden und den Prozessor so konfigurieren, dass er ein in diesem Kapitel beschriebenes Verfahren durchführt.

[0017] Bei einer besonders bevorzugten Ausführungsart der vorliegenden Erfindung sind die Zugangscodes Einmal-Authentifizierungscodes. Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung umfasst das Netz auch ein drahtloses Datenübertragungsnetz. Das Benutzergerät kann ein Mobiltelefon umfassen. Das Benutzergerät kann auch eine Smartcard umfassen. Bei einer besonders bevorzugten Ausführungsart der Erfindung handelt es sich bei den Nachrichten um SMS-Nachrichten.

[0018] Unter noch einem weiteren Aspekt wird im Folgenden eine Einrichtung zum Versorgen eines Benutzers mit einem Satz von Zugangscodes bereitgestellt, wobei die Einrichtung Folgendes umfasst: ein Benutzergerät; und einen Server zum Kommunizieren über ein Datenübertragungsnetz mit dem Benutzergerät; wobei das Benutzergerät Mittel zum Speichern eines kryptografischen Schlüssels und eines Kennungscodes und Mittel zum Senden einer Nachricht, welche den Kennungscode enthält, über das Netz an den Server umfasst; wobei der Server Mittel zum Speichern eines kryptografischen Schlüssels, welcher dem in dem Benutzergerät gespeicherten Schlüssel entspricht, Mittel zum Zuweisen des Satzes von Zugangscodes nach dem Empfang des Kennungscodes von dem Benutzergerät, Mittel zum Ausführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels vom Speicher, Mittel zum Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes; und Mittel zum Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät umfasst; und wobei das Benutzergerät ferner Mittel zum Entschlüsseln des vom Server empfangenen verschlüsselten Satzes mittels des in dem Benutzergerät gespeicherten Schlüssels und Mittel zum Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch den Benutzer umfasst.

[0019] Die vorliegende Erfindung erstreckt sich außerdem auf ein Benutzergerät zum Empfangen eines Satzes von Zugangscodes über ein Datenübertragungsnetz von einem Server, wobei das Gerät Folgendes umfasst: Mittel zum Speichern eines kryptografischen Schlüssels und eines Kennungscodes; Mittel zum Senden einer Nachricht, welche den Kennungscode enthält, über ein Datenübertragungsnetz an einen Server; Mittel zum Empfangen einer Nachricht, welche den Satz der mit dem Schlüssel verschlüsselten Zugangscodes enthält, vom Server; Mittel zum Entschlüsseln des empfangenen Satzes von Zugangscodes mittels des im Speicher gespeicherten Schlüssels; und Mittel zum Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes.

[0020] Außerdem erstreckt sich die vorliegende Erfindung auf einen Server zum Versorgen eines Benutzergerätes mit einem Satz von Zugangscodes über ein Datenübertragungsnetz, wobei der Server Folgendes umfasst: Mittel zum Speichern eines kryptografischen Schlüssels, welcher einem in dem Benutzergerät gespeicherten kryptografischen Schlüssel entspricht; Mittel zum Zuweisen des Satzes von Zugangscodes zum Benutzergerät nach dem Empfang einer Nachricht, welche einen Kennungscode enthält, über das Netz von dem Benutzergerät; Mittel zum Ausführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels aus dem Speicher; Mittel zum Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes; und Mittel zum Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät.

[0021] Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung wird ein sicheres Transaktionssystem bereitgestellt, das sowohl für Kunden als auch beispielsweise für Bankdienstleister gegenüber herkömmlichen Systemen sicherer und bequemer ist. Eine besonders bevorzugte Ausführungsart der

vorliegenden Erfindung umfasst: eine Smartcard, auf welcher eine oder mehrere Abstreichlisten manipulationssicher gespeichert sind; eine mobile Einrichtung zum bequemen Zugreifen auf die auf der Smartcard gespeicherten Abstreichlisten; und verschlüsselte Nachrichtenübermittlung über einen drahtlosen Datenübertragungskanal zwischen der mobilen Einrichtung und einem Servercomputer zum Aktualisieren der auf der Smartcard gespeicherten Abstreichlisten. Es ist von Vorteil, dass bezüglich der Sicherheit oder der Verschlüsselungsmöglichkeiten des drahtlosen Datenübertragungskanals keine Voraussetzungen geschaffen zu werden brauchen. Die mobile Einrichtung kann ein Mobiltelefon, ein PDA (Persönlicher Digitaler Assistent) oder Ähnliches sein. Die Smartcard kann ein SIM-Modul zum Einstecken in ein Mobiltelefon oder Ähnliches sein. Der drahtlose Datenübertragungskanal kann ein SMS-Kanal (Dienst für Kurzmitteilungen) oder ein GSM-Kanal (Globales System für Mobile Kommunikation) oder Ähnliches sein.

[0022] Bei einer besonders bevorzugten Ausführungsart der vorliegenden Erfindung, die hier kurz beschrieben wird, wird die mobile Einrichtung durch ein Mobiltelefon, die Smartcard durch ein SIM-Modul und der drahtlose Datenübertragungskanal durch einen SMS-Kanal in einem GSM-Netz implementiert. Bei dieser Ausführungsart ist der Kunde mit einem Mobiltelefon mit einem SIM-Modul ausgestattet. Das SIM-Modul umfasst eine Zentraleinheit (CPU) und einen Speicher. Java-kompatible Betriebssystemsoftware (Java ist ein Warenzeichen von Sun Microsystems) und Java-Toolkit-Appletsoftware sind im Speicher gespeichert. Die Betriebssystemsoftware konfiguriert die CPU zum Ausführen des Toolkits. Das Toolkit erleichtert die Bearbeitung von OTACs. Das Toolkit kann während der Einrichtung der SIM-Karte für den Kunden in den Speicher geladen werden. Alternativ kann das Toolkit, wenn der Dienstanbieter des GSM-Netzes dies zulässt, in den Speicher geladen und über das GSM-Netz dynamisch erneuert werden. Der Zugriff auf das Toolkit im Speicher ist durch eine persönliche Identifikationsnummer (PIN) geschützt, die der Kunde über das Mobiltelefon eingibt.

[0023] Bei einer besonders bevorzugten Ausführungsart der vorliegenden Erfindung sendet die Bank per Brief über den normalen Postweg ein Startdokument an den Kunden. Der Brief mit dem Startdokument enthält einen kundenspezifischen symmetrischen Schlüssel K, zum Beispiel einen 16-Byte-DES-Schlüssel; einen Kunden-Kennungscode (Identifizierungscode, ID) N; und eine Telefonnummer für einen SMS-kompatiblen Server bei der Bank. Der ID-Code N dient der Bank zum Identifizieren des Kunden. Der ID-Code braucht nicht gleich der Kontonummer des Kunden zu sein, sondern kann durch eine eindeutige Zufallsinformation implementiert werden.

[0024] Bei der erstmaligen Aktivierung durch den Kunden fordert das Toolkit den Kunden zur Eingabe des Schlüssels K, der Information N und der Telefonnummer des Servers über die Tastatur des Mobiltelefons auf. Dann sendet das Toolkit als SMS eine Initialisierungsnachricht, welche den Kennungscode N enthält, an den Server. Die Initialisierungsnachricht zeigt an, dass das Toolkit aktiviert ist. Der Server reagiert auf den Empfang der Initialisierungsnachricht, indem er an den Kunden als SMS eine Antwortnachricht sendet, welche eine Liste von mit dem Schlüssel K verschlüsselten OTACs enthält. Die OTAC-Liste kann sich je nach der zu übertragenden Datenmenge über mehrere SMS-Nachrichten erstrecken. Das Toolkit entschlüsselt die empfangene OTAC-Liste mittels des Schlüssels K. Dann ist die Initialisierung abgeschlossen. Wenn der Kunde einen OTAC benötigt, um beispielsweise über das Internet eine Transaktion im Onlinebanking durchzuführen, gibt er wieder die PIN in das Mobiltelefon ein, um das Toolkit freizugeben, und fordert vom Toolkit in Abhängigkeit von dem OTAC-Zuweisungssystem der Bank den nächsten oder einen bestimmten OTAC an. Das Toolkit überwacht die ausgegebenen OTACs. Wenn alle durch das Toolkit gespeicherten OTACs ausgegeben worden sind, wird vom Server eine neue OTAC-Liste empfangen. Die neue Liste wird wie oben beschrieben wiederum über den SMS-Kanal zugestellt. Der Server überwacht auch, wie viele und welche OTACs zu jedem Zeitpunkt von jedem Kunden benutzt wurden, und startet bei Bedarf automatisch die Aktualisierung. Man beachte, dass es bei diesem System nur eine Endpunt-zu-Endpunkt-Verschlüsselung zwischen dem Server und dem Toolkit im SIM-Modul des Kunden gibt. Bezüglich der Sicherheit des genutzten Funkkanals brauchen keine Voraussetzungen geschaffen zu werden.

[0025] Bei einer anderen bevorzugten Ausführungsart der vorliegenden Erfindung kann der Schlüssel K auf Anforderung durch das Senden eines neuen Schlüssels K', der mit dem Schlüssel K verschlüsselt ist, vom Server über den Funkkanal an das Toolkit aktualisiert werden. Daraufhin akzeptiert das Toolkit nur Nachrichten, die mit dem neuen Schlüssel K' verschlüsselt wurden. Die Verbreitung des neuen Schlüssels K' kann mit der Verbreitung der neuen OTAC-Listen erfolgen. Alternativ kann die Verbreitung des neuen Schlüssels K' unabhängig von der Verbreitung der neuen OTAC-Liste erfolgen.

[0026] Bei noch einer anderen bevorzugten Ausführungsart der vorliegenden Erfindung kann der Server einen anderen Schlüssel S, der mit dem Schlüssel K verschlüsselt wurde, über den Funkkanal an das Toolkit senden. Der andere Schlüssel S kann zum Beispiel zur Signaturprüfung benutzt werden. Dann werden weitere Nachrichten vom Server vor dem Verschlüsseln mit dem Schlüssel K mit dem Signaturschlüssel S signiert. Somit kann das Toolkit dann die

Signatur prüfen.

[0027] Bei einer weiteren Ausführungsart der vorliegenden Erfindung wird anstelle der oben beschriebenen symmetrischen Verschlüsselung eine asymmetrische Verschlüsselung praktiziert. In diesem Fall braucht der Kunde den ersten symmetrischen Schlüssel K nicht manuell einzugeben. Stattdessen erzeugt das Toolkit im SIM-Modul ein Paar öffentlicher/privater Schlüssel, wie beispielsweise ein 1024-Bit-RSA-Schlüsselpaar. Dann aktiviert sich das Toolkit, indem es den öffentlichen Schlüssel E Zusammen mit dem ID-Code N über den Datenübertragungskanal an den Server sendet. Für jede Nachricht an das Toolkit erzeugt der Server jetzt einen symmetrischen Sitzungsschlüssel. In jedem Fall verschlüsselt der Server die Nachricht mit dem sicheren Sitzungsschlüssel, verschlüsselt den Sitzungsschlüssel mit dem öffentlichen Schlüssel E und sendet die verschlüsselte Nachricht zusammen mit dem verschlüsselten Sitzungsschlüssel über den Funkkanal an das Toolkit. Das Toolkit entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel D. Dann entschlüsselt das Toolkit die oder jede andere Nachricht mittels des entschlüsselten Sitzungsschlüssels, um die OTAC-Liste wiederherzustellen.

[0028] Der Server kann zum Erzeugen und Prüfen der Signatur auch ein Paar öffentlicher/privater Schlüssel benutzen, indem er seinen öffentlichen Schlüssel für zukünftige Prüfungen an das Toolkit sendet. Man beachte, dass der Server zur Signaturprüfung an alle Toolkits ein und denselben öffentlichen Schlüssel ausgeben kann, der möglicherweise durch eine zusätzliche sichere Zertifizierungsinstanz signiert ist, welche über einen vorher auf der Smartcard gespeicherten öffentlichen Schlüssel verfügt.

[0029] Bei einer weiteren Ausführungsart der vorliegenden Erfindung umfasst mindestens eine mobile Einrichtung oder die Smartcard eine berührungslose Schnittstelle, wie beispielsweise eine Infrarot- oder Induktionsschnittstelle. Die Schnittstelle gestattet über ein Datenterminal den Zugriff auf das Toolkit auf der Smartcard. Nach dem Ausgeben einer Anforderung vom Kunden über das Datenterminal können über die Schnittstelle OTACs gelesen werden. Eine solche Anforderung kann zum Beispiel über eine Tastatur des Datenterminals ausgegeben werden. Alternativ können OTACs ohne die manuelle Ausgabe solcher Anforderungen über die Schnittstelle gelesen werden. Zwischen der Smartcard und dem Datenterminal können verschiedene Abfrage- und Antwortprozeduren benutzt werden. Zum Beispiel kann das Datenterminal selbst möglicherweise nicht in der Lage sein, auf den OTAC zuzugreifen. Stattdessen kann das Datenterminal eine Abfrage an das Toolkit senden. Das Toolkit wiederum erzeugt entsprechend dem OTAC eine Antwort auf die Abfrage. Wenn der OTAC wirklich einen kryptografischen Schlüssel, wie beispielsweise einen 3-DES-Schlüssel, umfasst, kann das Toolkit die Abfrage mit dem OTAC digital signieren und/oder verschlüsseln. Die somit berechnete Antwort kann zur Authentifizierung oder zur Freigabe einer Transaktion benutzt werden.

[0030] Es ist klar, dass die vorliegende Erfindung viele Vorteile bietet. Ein Vorteil der vorliegenden Erfindung besteht darin, dass sie ein sicheres Verfahren zum Verbreiten von OTACs an Benutzergeräte bereitstellt. Beispiele solcher Benutzergeräte sind unter anderem mobile Einrichtungen, die mit manipulationssicherer Smartcardtechnologie ausgerüstet sind und dennoch immer und überall einen bequemen Zugriff auf OTACs gestatten. Solch ein Zugriff kann entweder manuell oder über einen Funkkanal automatisch ausgelöst werden. Die vorliegende Erfindung ist insbesondere für Bankanwendungen attraktiv, da keine Änderungen an den üblicherweise in Banken verwendeten Computerinfrastrukturen erforderlich sind. Die Verbreitung von OTAC-Listen wird billiger, einfacher und sicherer durchgeführt. Darüber hinaus ist unter der Verwendung der vorhandenen Infrastruktur zu verstehen, dass dem Kunden keine zusätzlichen OTAC-spezifischen mobilen Einrichtungen und/oder Smartcards zur Verfügung gestellt werden müssen, wenn dieser bereits ein Mobiltelefon mit einer SIM-Karte besitzt, mit welchem Toolkit-Applets heruntergeladen und ausgeführt werden können.

[0031] Im Folgenden werden bevorzugte Ausführungsarten der vorliegenden Erfindung lediglich als Beispiel unter Bezug auf die beiliegenden Zeichnungen beschrieben, in denen:

[0032] Fig. 1 ein Blockdiagramm eines Datenverarbeitungsnetzes ist;

[0033] Fig. 2 ein Blockdiagramm einer Smartcard des Netzes ist;

[0034] Fig. 3 ein Blockdiagramm einer mobilen Einrichtung des Netzes ist;

[0035] Fig. 4 ein Blockdiagramm eines Server-Computersystems des Netzes ist;

[0036] Fig. 5 ein Flussdiagramm für die Smartcard ist;

[0037] Fig. 6 ein Blockdiagramm eines Speichers der Smartcard ist;

[0038] Fig. 7 ein Flussdiagramm für den Server ist;

[0039] Fig. 8 ein weiteres Flussdiagramm für die Smartcard ist;

[0040] Fig. 9 ein weiteres Blockdiagramm des Smartcardspeichers ist;

[0041] Fig. 10 noch ein weiteres Flussdiagramm für die Smartcard ist;

[0042] Fig. 11 ein weiteres Flussdiagramm für die Erneuerung der im Speicher der Smartcard gespeicherten OTACs ist;

[0043] Fig. 12 noch ein weiteres Flussdiagramm für den Server ist;

[0044] Fig. 13 ein weiteres Flussdiagramm für die Smartcard ist;

[0045] Fig. 14 noch ein weiteres Flussdiagramm für die Smartcard ist;

[0046] Fig. 15 ein weiteres Flussdiagramm für den Server ist;

[0047] Fig. 16 ebenfalls ein Flussdiagramm für die Smartcard ist; und

[0048] Fig. 17 ein Blockdiagramm eines Datenverarbeitungssystems ist, welches die vorliegende Erfindung realisiert.

[0049] Ein Datenverarbeitungsnetz von Fig. 1, welches die vorliegende Erfindung realisiert, umfasst ein Benutzergerät **100** in Form eines Mobiltelefons, das über eine Datenübertragungsnetzinfrastruktur **300** mit einem Funknetz in Form eines GSM-Netzes mit einem Server-Computersystem **200** verbunden werden kann. Über das Benutzergerät **100** kann auch eine Smartcard **10** in Form einer SIM-Karte mit dem Netz verbunden werden.

[0050] Fig. 2 zeigt, dass die Smartcard **10** einen Speicher **20**, eine Zentraleinheit (Central Processing Unit, CPU) **30**, eine Verschlüsselungseinheit **90** und ein Eingabe-/Ausgabe(E/A)-Subsystem **40** umfasst, die sämtlich über ein Bussubsystem **50** miteinander verbunden sind. Im Speicher **20** ist ein Computerprogrammcode gespeichert, der durch die CPU **30** ausgeführt werden kann. Der Computerprogrammcode umfasst ein Betriebssystem in Form einer Java-kompatiblen Betriebssystemplattform und ein Anwendungssoftware-Toolkit **70** in Form eines Java-Applets. Der Speicher **20** ermöglicht auch die manipulationssichere Speicherung einer Abstreichliste **80**. Die Abstreichliste **80** umfasst eine Vielzahl von OTACs. Das Betriebssystem **60** konfiguriert die CPU **30** zum Ausführen des Toolkits **70**. Das Toolkit **70** erleichtert die Verarbeitung von OTACs in der Abstreichliste **80**. Im Folgenden werden ausführlich Aspekte der Funktionalität des Toolkits **70** beschrieben. Die Verschlüsselungseinheit **280** umfasst eine kryptografische Verarbeitungslogik zum Verschlüsseln und Entschlüsseln von Daten, die durch die Smartcard **10** gesendet und empfangen werden. Die kryptografische Verarbeitungslogik kann in Form von Hardware, Software oder einer Kombination von Hard- und Software implementiert werden.

[0051] Gemäß Fig. 3 umfasst das Benutzergerät **100** eine Hochfrequenzstufe (HR-Stufe) **110** mit einer HF-Antenne **170**, eine Steuerlogik **130**, eine Bildschirmanzeige **140** und einen Tastenblock **160**, die sämtlich durch ein Bussubsystem **120** miteinander verbunden sind. Die Smartcard **10** ist entnehmbar in das Benutzergerät **100** eingesteckt und das E/A-Subsystem **40** der Smartcard **10** ist trennbar mit dem Bussubsystem **120** des Benutzergerätes **100** verbunden. Beim Betrieb erleichtern die HF-Stufe **110** und die HF-Antenne die drahtlose Datenübertragung zwischen dem Benutzergerät **100** und anderen mit dem Netz **300** verbundenen Einrichtungen. Die Bildschirmanzeige **140** stellt eine grafische Benutzeroberfläche zwischen dem Benutzer und den mobilen Einrichtungen für solche Funktionen wie das Vorbereiten und Lesen von Nachrichten dar. Der Tastenblock **160** stellt dem Benutzer eine Tastatursteuerung des Benutzergerätes **10** für solche Funktionen wie Dateneingabe und Anrufbehandlung zur Verfügung. Die Steuerlogik **130** steuert solche Funktionen des Benutzergerätes **100** wie die Anrufbehandlung entsprechend den zum Beispiel vom Tastenblock **160** empfangenen Eingaben. Die Ausgaben von dem Benutzergerät **100**, wie beispielsweise Datenanzeigen auf der Bildschirmanzeigeeinheit **140** oder über die HF-Stufe **110** abgehende Anrufe, werden ebenfalls durch die Steuerlogik **130** gesteuert. Desgleichen koordiniert die Steuerlogik **130** Datenübertragungen von der Smartcard **10** und den anderen Elementen des Benutzergerätes **100** über das Bussubsystem **120**. Die Steuerlogik **130** kann als spezielle Hardware, eine programmierte. CPU oder eine Kombination aus einer speziellen Hardware und einer programmierten CPU implementiert werden.

[0052] Gemäß Fig. 4 umfasst der Server **200** einen Speicher **210**, eine CPU **220** und ein E/A-Subsystem **230**, die sämtlich durch ein Bussubsystem **240** miteinander verbunden sind. Im Speicher **210** ist ein Computerprogrammcode gespeichert, der durch die CPU **220** ausgeführt werden kann. Der Computerprogrammcode umfasst ein Betriebssystem **250** und eine OTAC-Dienst-Anwendungssoftware **260**. Das Betriebssystem **250** konfiguriert die CPU **220** zum Durchführen des OTAC-Dienstes **260**. Der OTAC-Dienst **260** erleichtert die Behandlung von OTACs in dem Benutzergerät **100**. Im Folgenden werden ausführlich Aspekte der Funktionalität des OTAC-Dienstes **260** beschrieben.

[0053] Beim Betrieb wird zwischen dem Benutzergerät **100** und dem Server **200** ein drahtloser Datenübertragungskanal in Form eines SMS-Kanals aufgebaut. Der SMS-Kanal erleichtert die sichere Übertragung der Abstreichliste **80** vom OTAC-Dienst **260** im Server **200** über das Benutzergerät **100** zur Smart-

card **10**. Das Toolkit **70** kann während der Konfiguration der Smartcard **10** für den Benutzer in den Speicher **20** des Benutzergerätes **100** geladen werden. Alternativ kann das Toolkit **70**, wenn die Netzinfrastruktur **300** dies zulässt, in den Speicher **20** geladen und über die Netzinfrastruktur **300** dynamisch erneuert werden. Der Zugriff auf das Toolkit **70** im Speicher **20** ist durch eine PIN geschützt, die der Benutzer über das Benutzergerät **100** eingibt. Zu diesem Zweck kann der Tastaturblock **160** verwendet werden. Wenn das Benutzergerät **100** über eine Spracherkennung verfügt, kann die PIN mündlich eingegeben und gelöscht werden. Andere Einrichtungen können auch noch andere Dateneingabemittel unterstützen.

[0054] Bei einer besonders bevorzugten Ausführungsart der vorliegenden Erfindung befindet sich der Server **200** in einer Bank und der Benutzer des Benutzergerätes **100** ist ein Kunde der Bank. Zuerst sendet die Bank dem Benutzer einen Postbrief. Der Postbrief kann zum Beispiel über das normale Postsystem geschickt werden. Der Postbrief enthält: einen kundenspezifischen symmetrischen Schlüssel K, wie beispielsweise einen 16-Byte-DES-Schlüssel; einen Kundenkennungscode (ID) N; und eine Telefonnummer zum Zugreifen auf den Server **200** über die Netzinfrastruktur **300**. Die Bank verwendet den ID-Code N zur Identifizierung des Benutzers. Der ID-Code braucht nicht gleich der Kundenkontonummer des Benutzers zu sein, sondern kann statt dessen durch eine eindeutige Zufallsinformation implementiert werden.

[0055] Zur erstmaligen Aktivierung des Toolkits **70** gemäß Fig. 5 gibt der Benutzer in Schritt **400** über den Tastenblock **160** die PIN ein. Nach dem Empfang der PIN fordert das Toolkit **70** in Schritt **410** den Benutzer zum Eingeben des Schlüssels K, des ID-Codes N und der Telefonnummer des Servers **200** über den Tastenblock **160** auf. Wenn das Benutzergerät **100** wie oben erwähnt über eine Spracherkennung verfügt, können diese Daten auch mündlich eingegeben werden. Es ist jedoch klar, dass dies Verfahren weniger sicher ist, da der Benutzer beim Ansagen der Daten abgehört werden kann. Nach dem Empfang der oben angegebenen Benutzerdaten sendet das Toolkit **70** in Schritt **420** zur Initialisierung eine SMS-Nachricht, welche den Kennungscode N enthält, an den OTAC-Dienst **260** auf dem Server **200**. Die Initialisierungsnachricht zeigt dem OTAC-Dienst **260** an, dass das Toolkit **70** aktiviert wurde. Gemäß Fig. 6 enthält der Speicher **20** auf der Smartcard nun die PIN, den Schlüssel K und den ID-Code N.

[0056] Nach dem Empfang der Initialisierungsnachricht im Server **200** sucht der OTAC-Dienst **260** gemäß Fig. 7 in Schritt **430** anhand des ID-Codes N nach dem Benutzer und ruft den an den Benutzer ausgegebenen Schlüssel K ab. Dann verschlüsselt der OTAC-Dienst **260** in Schritt **440** mit dem Schlüssel K eine neue Abstreichliste mit OTACs für den Benutzer. Dann sendet der OTAC-Dienst **260** eine SMS-Antwortnachricht, welche die verschlüsselte Liste enthält, an das Toolkit **70**. Die Liste kann sich je nach der zu übertragenden Datenmenge auf eine Reihe von SMS-Nachrichten erstrecken.

[0057] Nach dem Empfang der Antwortnachricht in dem Benutzergerät **100** extrahiert das Toolkit **70** gemäß Fig. 8 in Schritt **460** die verschlüsselte Liste. Das Toolkit **70** nutzt zur Entschlüsselung der Liste in Schritt **470** mittels des Schlüssels K die Verschlüsselungseinheit **90**. Dann speichert das Toolkit **70** in Schritt **480** die entschlüsselte Liste im Speicher **60**. Damit ist die Initialisierung abgeschlossen. Nun enthält der Speicher **20** gemäß Fig. 9 den Schlüssel K, die PIN, den ID-Code N und die OTAC-Liste.

[0058] Wenn der Benutzer zum Ausführen einer Banktransaktion zum Beispiel über das Internet einen OTAC benötigt, gibt der Benutzer gemäß Fig. 10 in Schritt **500** über den Tastenblock **160** die PIN ein, um das Toolkit **70** zu entsperren. Dann fordert der Benutzer in Schritt **510** einen OTAC vom Toolkit **70** an, wobei der OTAC je nach dem von der Bank verwendeten OTAC-Zuweisungssystem der nächste oder ein bestimmter OTAC in der Liste sein kann. Das Toolkit **70** überwacht in Schritt **520** die ausgegebenen OTACs.

[0059] Zum Erneuern der im Speicher **20** gespeicherten OTAC-Liste **80** können viele Verfahren verwendet werden. Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung zum Beispiel wird die Erneuerung der OTAC-Liste **80** automatisch durch das Toolkit **70** ausgelöst. Insbesondere führt das Toolkit **70** gemäß Fig. 11 bei jeder Verwendung eines OTACs in Schritt **530** eine Prüfung in Schritt **540** durch, um zu ermitteln, ob die Anzahl der restlichen unbenutzten OTACs in der Liste **80** einen vorgegebenen Schwellenwert unterschreitet. Falls die Anzahl der unbenutzten OTACs den Schwellenwert überschreitet, wartet das Toolkit **70** auf den nächsten OTAC, der benutzt werden soll. Wenn jedoch der Schwellenwert erreicht wurde, erzeugt das Toolkit **70** automatisch eine Nachricht und sendet diese über das Netz **300** an den Server **200**, um eine neue OTAC-Liste anzufordern. Die Anforderungsnachricht enthält, wie oben unter Bezug auf Fig. 5 beschrieben, den ID-Code N, damit der OTAC-Dienst **260** im Server **200** nach dem passenden Schlüssel zum Verschlüsseln der neuen OTAC-Liste suchen kann. Die neue Liste wird dann, wie oben unter Bezug auf Fig. 7 beschrieben, über den Kanal an die Smartcard **10** gesendet. Bei einer anderen Ausführungsart der vorliegenden Erfindung wird die im Speicher **20** gespeicherte OTAC-Liste **80** automatisch durch den OTAC-Dienst **260** auf dem Server **200** erneuert. Dabei überwacht der OTAC-Dienst **260** auf dem Server

200 nun gemäß Fig. 11 in Schritt **530**, wie viele und welche OTACs zu welchem Zeitpunkt von jedem Benutzer benutzt worden sind. Jedes Mal, wenn ein OTAC benutzt wird, ermittelt der OTAC-Dienst **260** in Schritt **540**, ob die Anzahl der restlichen unbenutzten OTACs in der Liste einen vorgegebenen Schwellenwert unterschreitet. Wenn dies nicht der Fall ist, wartet der OTAC-Dienst **260** auf den nächsten OTAC, der benutzt werden soll. Wenn dies jedoch der Fall ist, sendet der OTAC-Dienst **260**, wie oben unter Bezug auf

[0060] Fig. 7 beschrieben, automatisch eine neue mit dem Schlüssel K verschlüsselte Liste an das Toolkit **70**. Die oben beschriebenen Schwellenwerte können so gewählt werden, dass eine neue Liste **80** ausgegeben wird, wenn alle zuvor ausgegebenen OTACs verbraucht sind. Alternativ können die Schwellenwerte so gewählt werden, dass eine neue Liste **80** ausgegeben wird, wenn in der vorherigen Liste nur eine vorgegebene Anzahl noch unbenutzter OTACs übrig ist. Bei noch einer anderen Ausführungsart der vorliegenden Erfindung kann die Erneuerung der im Speicher **20** gespeicherten OTAC-Liste **80** manuell durch den Benutzer ausgelöst werden. Dabei erzeugt das Toolkit **70** insbesondere als Reaktion auf eine manuelle Eingabe in das Benutzergerät **100** eine Nachricht und sendet diese über das Netz **300** an den Server **200**, um eine neue OTAC-Liste anzufordern. Die oben unter Bezug auf Fig. 5 beschriebene Antwortnachricht enthält den ID-Code N, damit der OTAC-Dienst **260** im Server **200** nach dem passenden Schlüssel zum Verschlüsseln der neuen OTAC-Liste suchen kann. Auch in diesem Fall wird die neue Liste, wie oben unter Bezug auf Fig. 7 beschrieben, über den Kanal an die Smartcard **10** gesendet. Man beachte, dass bei diesen Erneuerungssystemen nur eine Endpunktzu-Endpunkt-Verschlüsselung zwischen dem OTAC-Dienst **260** und dem Toolkit **70** stattfindet. Bezüglich der Sicherheit der beteiligten Netzinfrastruktur **300** brauchen keine Voraussetzungen geschaffen zu werden.

[0061] Bei einer Variante der oben unter Bezug auf die Fig. 5 bis Fig. 11 beschriebenen bevorzugten Ausführungsart der vorliegenden Erfindung kann der im Speicher **20** gespeicherte Schlüssel K auf Anforderung aktualisiert werden. Dabei erzeugt der OTAC-Dienst **260** gemäß Fig. 12 in Schritt **550** einen neuen Schlüssel K'. Der OTAC-Dienst **260** verschlüsselt den neuen Schlüssel K' in Schritt **560** mit dem bereits vorhandenen Schlüssel K. Dann sendet der OTAC-Dienst **260** eine SMS-Nachricht mit dem durch den vorhandenen Schlüssel K verschlüsselten neuen Schlüssel K' über die Netzinfrastruktur **300** an das Toolkit **70**.

[0062] Das Toolkit **70** empfängt gemäß Fig. 13 in Schritt **600** den verschlüsselten neuen Schlüssel K'. Das Toolkit **70** entschlüsselt den neuen Schlüssel K' in Schritt **610** mittels des zuvor im Speicher **20** gespeicherten Schlüssel K mit Hilfe der Verschlüsselungseinheit **280**. Dann ersetzt das Toolkit **70** den zuvor vorhandenen Schlüssel K im Speicher **20** durch den neuen Schlüssel K'. Danach akzeptiert das Toolkit **70** nur noch Nachrichten, die mit dem neuen Schlüssel K' verschlüsselt sind. Die Verbreitung des neuen Schlüssels K' kann zusammen mit der Verbreitung der neuen Listen durch den Server **200** erfolgen. Alternativ kann die Verbreitung des neuen Schlüssels K' unabhängig von der Verbreitung der neuen Listen erfolgen.

[0063] Bei einer anderen Variante der oben unter Bezug auf die Fig. 5 bis Fig. 11 beschriebenen bevorzugten Ausführungsart der vorliegenden Erfindung sendet der OTAC-Dienst **260** einen anderen mit dem Schlüssel K verschlüsselten Schlüssel S über die Netzinfrastruktur **300** an das Toolkit **70**. Der andere Schlüssel S kann zum Beispiel zur Signaturprüfung eingesetzt werden. Spätere Nachrichten vom OTAC-Dienst **260** werden dann vor dem Verschlüsseln mit dem Schlüssel K mit dem Signaturschlüssel S signiert. Dann kann das Toolkit **70** die Signatur entsprechend prüfen. Die Schlüssel K und S brauchen nicht unbedingt verschieden zu sein.

[0064] Bei der oben beschriebenen bevorzugten Ausführungsart der vorliegenden Erfindung wird die symmetrische Verschlüsselung verwendet. Bei einer anderen Ausführungsart der vorliegenden Erfindung wird jedoch die asymmetrische Verschlüsselung verwendet. Bei dieser Ausführungsart braucht der Benutzer den ersten symmetrischen Schlüssel K nicht manuell einzugeben. Statt dessen erzeugt das Toolkit **70** gemäß Fig. 14 in Schritt **630** mit Hilfe der Verschlüsselungseinheit **280** ein Paar öffentlicher/privater Schlüssel, wie beispielsweise ein 1024-Bit-RSA-Schlüsselpaar. Dann sendet das Toolkit **70** in Schritt **640** den öffentlichen Schlüssel E des Paars zusammen mit dem ID-Code N über die Netzinfrastruktur **300** an den OTAC-Dienst **260**. Nun ist das Toolkit **70** aktiviert.

[0065] Nun erzeugt der OTAC-Dienst **260** gemäß Fig. 15 in Schritt **650** einen sicheren symmetrischen Sitzungsschlüssel P. In Schritt **660** erzeugt der OTAC-Dienst **260** eine Nachricht, welche eine OTAC-Liste enthält. Nun verschlüsselt der OTAC-Dienst **260** die Nachricht in Schritt **670** mit dem Sitzungsschlüssel P. Der OTAC-Dienst **260** verschlüsselt in Schritt **680** auch den Sitzungsschlüssel P mit dem öffentlichen Schlüssel E. Dann sendet der OTAC-Dienst **260** in Schritt **690** die verschlüsselte Nachricht zusammen mit dem verschlüsselten Sitzungsschlüssel P über die Netzinfrastruktur **300** an das Toolkit **70**.

[0066] Das Toolkit **70** entschlüsselt gemäß Fig. 16 in Schritt **700** den Sitzungsschlüssel P mittels seines

privaten Schlüssels D mit Hilfe der Verschlüsselungseinheit **280**. Dann entschlüsselt das Toolkit **70** in Schritt **710** die Nachricht mittels des entschlüsselten Sitzungsschlüssels mit Hilfe der Verschlüsselungseinheit **280**. Dann stellt das Toolkit **70** in Schritt **720** aus der entschlüsselten Nachricht die Liste wieder her.

[0067] Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung benutzt der OTAC-Dienst **260** auch ein Paar öffentlicher/privater Schlüssel zum Erzeugen und Prüfen von Signaturen. Der OTAC-Dienst **260** sendet seinen öffentlichen Schlüssel für zukünftige Prüfungen an das Toolkit **70**. Man beachte, dass der OTAC-Dienst **260** denselben öffentlichen Schlüssel zur Signaturprüfung an alle durch ihn versorgten Toolkits **70** ausgeben kann, der möglicherweise durch eine sichere externe Zertifizierungsinstanz signiert ist, die über einen zuvor auf der Smartcard **10** gespeicherten öffentlichen Schlüssel verfügt.

[0068] Bei einer anderen Ausführungsart der vorliegenden Erfindung umfasst das Benutzergerät **100** gemäß Fig. 17 eine berührungslose Schnittstelle **800**, wie beispielsweise eine Infrarot- oder Induktionsschnittstelle. Die Schnittstelle **800** erlaubt den Zugriff über ein Datenterminal **810** auf das Toolkit **70** auf der Smartcard **10**. Das Datenterminal **810** umfasst auch eine berührungslose Schnittstelle **880** zum Kommunizieren mit der Schnittstelle **800** des Benutzergerätes **100**. Das Datenterminal **800** umfasst ferner einen Tastenblock **830**, eine Anzeigevorrichtung **840** und ein E/A-Subsystem **850**, die sämtlich über ein Bussubsystem **820** mit der Schnittstelle **880** verbunden sind. Das E/A-Subsystem **850** ist über ein beteiligtes Datennetz **860** mit einem fernen Transaktionsverarbeitungs-Computersystem **870** verbunden.

[0069] Beim Betrieb können als Reaktion auf eine durch den Kunden über den Tastenblock **830** des Datenterminals **810** ausgegebene Anforderung OTACs durch das Datenterminal **810** über die Schnittstellen **800** und **880** von der in dem Benutzergerät **100** befindlichen Smartcard **10** gelesen werden. Alternativ können OTACs durch das Datenterminal **810** über die Schnittstellen **800** und **880** gelesen werden, ohne dass solche manuellen Anforderungen erforderlich sind. Zwischen der Smartcard **10** und dem Datenterminal **810** können verschiedene Abfrage- und Antwortprozeduren verwendet werden.

[0070] Bei einer bevorzugten Ausführungsart der vorliegenden Erfindung kann das Datenterminal **810** zum Beispiel nicht auf die OTACs zugreifen. Statt dessen sendet das Datenterminal **810** eine Abfrage an das Toolkit **70** in der Smartcard **10**. Das Toolkit **70** wiederum erzeugt anhand des OTAC eine Antwort auf die Abfrage. Wenn der OTAC zum Beispiel einen kryptografischen Schlüssel, wie beispielsweise einen 3-DES-Schlüssel, umfasst, kann das Toolkit **70** die Abfrage mit dem OTAC digital signieren und verschlüsseln.

[0071] Die somit berechnete Antwort kann zur Authentifizierung oder zur Freigabe einer Transaktion verwendet werden. Bei anderen Ausführungsarten der vorliegenden Erfindung kann die Schnittstelle **800** nicht Bestandteil des Benutzergerätes **100**, sondern Bestandteil der Smartcard **10** sein.

[0072] Bei den oben beschriebenen bevorzugten Ausführungsarten der vorliegenden Erfindung wird das Benutzergerät **100** in Form eines Mobiltelefons verwendet. Bei anderen Ausführungsarten der vorliegenden Erfindung kann das Benutzergerät **100** jedoch auch in anderer Form verwendet werden, zum Beispiel als PDA, als tragbarer Computer, als Arbeitsplatzcomputer oder Ähnliches. Desgleichen wird bei den oben beschriebenen bevorzugten Ausführungsarten der vorliegenden Erfindung zur Datenübertragung zwischen dem Benutzergerät **100** und dem Server **200** ein drahtloses Netz verwendet. Bei anderen Ausführungsarten der vorliegenden Erfindung kann jedoch zur Datenübertragung zwischen dem Benutzergerät **100** und dem Server **200** ein leitungsgebundenes Netz oder eine Kombination aus drahtlosen und leitungsgebundenen Netzen verwendet werden. Außerdem erfolgt bei den oben beschriebenen bevorzugten Ausführungsarten der vorliegenden Erfindung die drahtlose Datenübertragung zwischen dem Benutzergerät **100** und dem Server **200** über einen SMS-Kanal. Bei anderen Ausführungsarten der vorliegenden Erfindung kann jedoch eine andere Form der Nachrichtenübermittlung verwendet werden. Außerdem wird bei den oben beschriebenen bevorzugten Ausführungsarten der vorliegenden Erfindung die Smartcard **10** in Form eines SIM-Moduls verwendet. Bei anderen Ausführungsarten der vorliegenden Erfindung kann die Smartcard **10** jedoch auch in anderer Form verwendet werden, zum Beispiel mit dem Formfaktor einer Kreditkarte oder einer Geldkarte. Anstelle der Smartcard **10** können analoge Formen spezieller Prozessorsysteme verwendet werden. Bei den Ausführungsarten der vorliegenden Erfindung wird in der Smartcard **10** ein Java-kompatibles Betriebssystem **60** zum Ausführen des Toolkits **70** in Form eines Java-Applets verwendet.

[0073] Bei anderen Ausführungsarten der vorliegende Erfindung kann jedoch eine andere Art von Betriebssystem für die Smartcard und eine entsprechend andere Art von Toolkit-Anwendungssoftware verwendet werden. Außerdem haben die Zugangscodes bei den bevorzugten Ausführungsarten der vorliegenden Erfindung die Form von Einmal-Authentifizierungscodes. Es ist jedoch klar, dass die vorliegende Erfindung auch auf die Zustellung von anderen Arten von Zugangscodes angewendet werden kann, zum Beispiel auf Zugangscodes zum Gewäh-

ren des Zutritts zu gesperrten Bereichen. Viele andere Anwendungen der vorliegenden Erfindung sind offensichtlich.

[0074] Insgesamt wurde oben als Beispiel der vorliegenden Erfindung ein Verfahren zum Bereitstellen eines Benutzergerätes mit einem Satz von Zugangscodes beschrieben, wobei das Verfahren in dem Benutzergerät das Speichern eines kryptografischen Schlüssels und eines Identifizierungscodes und das Senden einer Nachricht, welche den Identifizierungscode enthält, über ein Datenübertragungsnetz an einen Server umfasst. Im Server ist ein kryptografischer Schlüssel gespeichert, welcher dem in dem Benutzergerät gespeicherten Schlüssel entspricht, und der Server weist nach dem Empfang des Identifizierungscodes von dem Benutzergerät den Satz von Zugangscodes zu. Ausgehend von dem in der Nachricht empfangenen Identifizierungscode wird eine Suchfunktion ausgeführt, um den Schlüssel aus dem Speicher abzurufen. Der Satz der Zugangscodes wird mittels des abgerufenen Schlüssels verschlüsselt, sodass ein verschlüsselter Satz erzeugt wird. Eine Nachricht, welche den verschlüsselten Satz enthält, wird über das Netz an das Benutzergerät gesendet. In dem Benutzergerät wird der vom Server empfangene verschlüsselte Satz mittels des im Speicher befindlichen Schlüssels entschlüsselt und der entschlüsselte Satz der Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes gespeichert.

Patentansprüche

1. Verfahren zum Bereitstellen eines Benutzergerätes mit einem Satz von Zugangscodes, wobei das Verfahren Folgendes umfasst:
im Benutzergerät, Speichern eines kryptografischen Schlüssels und eines Kennungscodes und Senden einer Nachricht, welche den Kennungscode enthält, über ein Datenübertragungsnetz an einen Server;
im Server, Speichern eines kryptografischen Schlüssels, der dem in dem Benutzergerät gespeicherten Schlüssel entspricht, Zuweisen des Satzes von Zugangscodes nach dem Empfang des Kennungscodes von dem Benutzergerät, Durchführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels aus dem Speicher, Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes und Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät; und,
im Benutzergerät, Entschlüsseln des vom Server empfangenen verschlüsselten Satzes mittels des Schlüssels aus dem Speicher und Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes; und
Senden einer Nachricht, welche einen neuen Satz von Zugangscodes enthält, vom Server über das Netz an das Benutzergerät, wenn die Anzahl der unbenutzten Zugangscodes einen vorgegebenen Schwellenwert erreicht; und,
im Benutzergerät, Speichern des neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

2. Verfahren nach Anspruch 1, welches ferner Folgendes umfasst:
im Benutzergerät, Überwachen der durch den Benutzer verwendeten Zugangscodes, Erzeugen einer Anforderung als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes und Senden einer Nachricht, welche die Anforderung enthält, an den Server; und,
im Server, Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, nach dem Empfang der Anforderung.

3. Verfahren nach Anspruch 1, welches ferner Folgendes umfasst:
im Server, Überwachen der durch den Benutzer verwendeten Zugangscodes und Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, an das Benutzergerät als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes.

4. Verfahren nach Anspruch 1, welches ferner Folgendes umfasst:
im Server, Erzeugen eines neuen Schlüssels, Verschlüsseln des neuen Schlüssels mit dem vorherigen Schlüssel und Senden einer Nachricht, welche den verschlüsselten neuen Schlüssel enthält, über das Netz an das Benutzergerät; und,
im Benutzergerät, Entschlüsseln des vom Server empfangenen neuen Schlüssels mittels des vorherigen Schlüssels und Speichern des entschlüsselten neuen Schlüssels anstelle des vorherigen Schlüssels.

5. Verfahren nach Anspruch 4, welches ferner Folgendes umfasst:
im Server, Verschlüsseln eines neuen Satzes von Zugangscodes mit dem neuen Schlüssel zum Erzeugen eines mit dem neuen Schlüssel verschlüsselten Satzes und Senden einer Nachricht, welche den mit dem neuen Schlüssel verschlüsselten Satz enthält, über das Netz an das Benutzergerät; und,
im Benutzergerät, Entschlüsseln des mit dem neuen Schlüssel verschlüsselten Satzes mittels des neuen Schlüssels und Speichern des entschlüsselten neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

6. Verfahren nach Anspruch 1, welches ferner Folgendes umfasst:
im Benutzergerät, Erzeugen eines Paars öffentli-

cher/privater Schlüssel und Senden einer Nachricht, welche den öffentlichen Schlüssel des Paars enthält, über das Netz an den Server;
im Server, Erzeugen eines Sitzungsschlüssels, Verschlüsseln des Satzes von Zugangscodes mit dem Sitzungsschlüssel zum Erzeugen eines mit dem Sitzungsschlüssel verschlüsselten Satzes, Verschlüsseln des Sitzungsschlüssels mit dem öffentlichen Schlüssel zum Erzeugen eines verschlüsselten Sitzungsschlüssels, Senden einer Nachricht, welche den mit dem Sitzungsschlüssel verschlüsselten Satz und den verschlüsselten Sitzungsschlüssel enthält, über das Netz an das Benutzergerät; und,
im Benutzergerät, Entschlüsseln des verschlüsselten Sitzungsschlüssels mit dem privaten Schlüssel des Paars zum Wiederherstellen des Sitzungsschlüssels, Entschlüsseln des mit dem Sitzungsschlüssel verschlüsselten Satzes mit dem wiederhergestellten Sitzungsschlüssel zum Wiederherstellen des Satzes und Speichern des entschlüsselten Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

7. Verfahren zum Bereitstellen eines Benutzergerätes mit einem Satz von Zugangscodes, wobei das Verfahren im Benutzergerät Folgendes umfasst:
Speichern eines kryptografischen Schlüssels und eines Kennungscodes;
Senden einer Nachricht, welche den Kennungscode enthält, über ein Datenübertragungsnetz an einen Server;
Empfangen einer Nachricht, welche den Satz der mit dem Schlüssel verschlüsselten Zugangscodes enthält, vom Server;
Entschlüsseln des empfangenen Satzes von Zugangscodes mittels des im Speicher gespeicherten Schlüssels; und
Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes;
Empfangen einer Nachricht, welche einen neuen Satz von Zugangscodes enthält, vom Server nach dem Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes; und,
im Benutzergerät, Speichern des neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

8. Verfahren nach Anspruch 7, welches ferner Folgendes umfasst:
im Benutzergerät, Überwachen der durch den Benutzer benutzten Zugangscodes, Erzeugen einer Anforderung als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes und Senden einer Nachricht welche die Anforderung enthält, an den Server.

9. Verfahren nach Anspruch 7, welches im Benutzergerät ferner Folgendes umfasst:
Entschlüsseln eines vom Server empfangenen neuen Schlüssels mittels des vorherigen Schlüssels; und
Speichern des entschlüsselten neuen Schlüssels anstelle des vorherigen Schlüssels.

10. Verfahren nach Anspruch 9, welches im Benutzergerät Folgendes umfasst:
Empfangen einer Nachricht, welche einen mit dem neuen Schlüssel verschlüsselten Satz von Zugangscodes enthält, über das Netz vom Server;
Entschlüsseln des mit dem neuen Schlüssel verschlüsselten Satzes mittels des neuen Schlüssels; und
Speichern des entschlüsselten neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

11. Verfahren nach Anspruch 7, welches im Benutzergerät Folgendes umfasst:
Erzeugen eines Paars öffentlicher/privater Schlüssel;
Senden einer Nachricht, welche den öffentlichen Schlüssel des Paars enthält, über das Netz an den Server;
Empfangen einer Nachricht, welche einen mit einem Sitzungsschlüssel verschlüsselten Satz von Zugangscodes und einen mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel enthält, über das Netz vom Server;
Entschlüsseln des mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels mit dem privaten Schlüssel des Paars zum Wiederherstellen eines mit dem Sitzungsschlüssel verschlüsselten Satzes und eines entsprechenden Sitzungsschlüssels;
Entschlüsseln des mit dem Sitzungsschlüssel verschlüsselten Satzes mit dem wiederhergestellten Sitzungsschlüssel zum Wiederherstellen des Satzes; und
Speichern des entschlüsselten Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

12. Computerprogrammelement, welches Computerprogrammcodemittel umfasst, die in einen Prozessor eines Benutzergerätes geladen werden und den Prozessor so konfigurieren, dass er ein Verfahren nach einem der Ansprüche 7 bis 11 durchführt.

13. Verfahren zum Bereitstellen eines Benutzergerätes mit einem Satz von Zugangscodes, wobei das Verfahren in einem Server zum Kommunizieren über ein Netz mit dem Benutzergerät Folgendes umfasst:
Speichern eines kryptografischen Schlüssels, welcher einem im Benutzergerät gespeicherten kryptografischen Schlüssel entspricht;
Zuweisen des Satzes von Zugangscodes zum Benutzergerät nach dem Empfang einer Nachricht, welche einen Kennungscode enthält, über das Netz vom Benutzergerät;
Ausführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes, um den

Schlüssel vom Speicher abzurufen;
Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes; und
Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät; und
Senden einer Nachricht, welche einen neuen Satz von Zugangscodes enthält, über das Netz an das Benutzergerät nach dem Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes.

14. Verfahren nach Anspruch 13, welches im Server ferner Folgendes umfasst:
Erzeugen eines neuen Schlüssels, Verschlüsseln des neuen Schlüssels mit dem vorherigen Schlüssel; und
Senden einer Nachricht, welche den verschlüsselten neuen Schlüssel enthält, über das Netz an das Benutzergerät.

15. Verfahren nach Anspruch 14, welches im Server ferner Folgendes umfasst:
Verschlüsseln des neuen Satzes von Zugangscodes mit dem neuen Schlüssel zum Erzeugen eines mit dem neuen Schlüssel verschlüsselten Satzes von Zugangscodes.

16. Verfahren nach Anspruch 13, welches im Server ferner Folgendes umfasst:
Empfangen einer Nachricht, welche einen öffentlichen Schlüssel eines Paars öffentlicher/privater Schlüssel enthält, vom Benutzergerät;
Erzeugen eines Sitzungsschlüssels;
Verschlüsseln des Satzes von Zugangscodes mit dem Sitzungsschlüssel zum Erzeugen eines mit dem Sitzungsschlüssel verschlüsselten Satzes;
Verschlüsseln des Sitzungsschlüssels mit dem öffentlichen Schlüssel zum Erzeugen eines mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels; und
Senden einer Nachricht, welche den mit dem Sitzungsschlüssel verschlüsselten Satz und den mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel enthält, über das Netz an das Benutzergerät.

17. Computerprogrammelement, welches Computerprogrammcodemittel umfasst, die in einen Prozessor eines Servercomputersystems geladen werden und den Prozessor so konfigurieren, dass er ein Verfahren nach einem der Ansprüche 13 bis 16 durchführt.

18. Verfahren nach einem der Ansprüche 1 bis 16, bei welchem die Zugangscodes Einmal-Authentifizierungscodes sind.

19. Verfahren nach einem der Ansprüche 1 bis 16, oder 18, bei welchem das Netz ein drahtloses Datenübertragungsnetz umfasst.

20. Verfahren nach Anspruch 19, bei welchem das Benutzergerät ein Mobiltelefon, einen persönlichen digitalen Assistenten oder eine Smartcard umfasst.

21. Verfahren nach Anspruch 19, bei welchem die Nachrichten SMS-Nachrichten sind.

22. Einrichtung zum Bereitstellen eines Satzes von Zugangscodes für einen Benutzer, wobei die Einrichtung Folgendes umfasst:
ein Benutzergerät; und einen Server zum Kommunizieren über ein Datenübertragungsnetz mit dem Benutzergerät; wobei das Benutzergerät folgendes umfasst: Mittel zum Speichern eines kryptografischen Schlüssels und eines Kennungscodes und Mittel zum Senden einer Nachricht, welche den Kennungscode enthält, über das Netz an den Server; wobei der Server Folgendes umfasst: Mittel zum Speichern eines kryptografischen Schlüssels, welcher dem im Benutzergerät gespeicherten Schlüssel entspricht, Mittel zum Zuweisen des Satzes von Zugangscodes nach dem Empfang des Kennungscodes vom Benutzergerät, Mittel zum Ausführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels vom Speicher, Mittel zum Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes und Mittel zum Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät und zum Senden einer Nachricht, welche einen neuen Satz von Zugangscodes enthält, nach dem Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes über das Netz an das Benutzergerät; und, im Benutzergerät, Speichern des neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes, und
wobei das Benutzergerät ferner Folgendes umfasst: Mittel zum Entschlüsseln des vom Server empfangenen verschlüsselten Satzes mittels des im Benutzergerät gespeicherten Schlüssels und Mittel zum Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch den Benutzer.

23. Einrichtung nach Anspruch 22, bei welcher der Server ferner Folgendes umfasst:
Mittel zum Erzeugen eines neuen Schlüssels, Mittel zum Verschlüsseln des neuen Schlüssels mit dem vorherigen Schlüssel und Mittel zum Senden einer Nachricht, welche den verschlüsselten neuen Schlüssel enthält, über das Netz an das Benutzergerät, und bei welcher das Benutzergerät ferner Folgendes umfasst: Mittel zum Entschlüsseln des vom Server empfangenen neuen Schlüssels mittels des vorherigen Schlüssels und Mittel zum Speichern des entschlüsselten neuen Schlüssels anstelle des vor-

herigen Schlüssels.

24. Einrichtung nach Anspruch 23, bei welcher der Server ferner Folgendes umfasst:
Mittel zum Verschlüsseln des neuen Satzes von Zugangscodes mit dem neuen Schlüssel zum Erzeugen eines mit dem neuen Schlüssel verschlüsselten Satzes; und Mittel zum Senden einer Nachricht, welche den mit dem neuen Schlüssel verschlüsselten Satz enthält, über das Netz an das Benutzergerät, und bei welcher das Benutzergerät ferner Folgendes umfasst: Mittel zum Entschlüsseln des mit dem neuen Schlüssel verschlüsselten Satzes mittels des neuen Schlüssels und Mittel zum Speichern des entschlüsselten neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

25. Einrichtung nach Anspruch 22, welche ferner im Benutzergerät Mittel zum Speichern des neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes umfasst.

26. Einrichtung nach Anspruch 25, welche ferner Folgendes umfasst:
im Benutzergerät, Mittel zum Überwachen der durch den Benutzer benutzten Zugangscodes, Mittel zum Erzeugen einer Anforderung als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes und Mittel zum Senden einer Nachricht, welche die Anforderung enthält, an den Server; und, im Server, Mittel zum Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, nach dem Empfang der Anforderung.

27. Einrichtung nach Anspruch 25, welche ferner Folgendes umfasst:
im Server, Mittel zum Überwachen der durch den Benutzer benutzten Zugangscodes und Mittel zum Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, an das Benutzergerät als Reaktion auf das Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes.

28. Einrichtung nach Anspruch 25, welche ferner Folgendes umfasst:
im Benutzergerät, Mittel zum Erzeugen einer Anforderung als Reaktion auf eine manuelle Eingabe vom Benutzer und Mittel zum Senden einer Nachricht, welche die Anforderung enthält, an den Server; und, im Server, Mittel zum Senden der Nachricht, welche den neuen Satz von Zugangscodes enthält, nach dem Empfang der Anforderung.

29. Einrichtung nach Anspruch 22, bei welcher das Benutzergerät ferner Folgendes umfasst:
Mittel zum Erzeugen eines Paars öffentlicher/privater Schlüssel und Mittel zum Senden einer Nachricht, welche den öffentlichen Schlüssel des Paars enthält, über das Netz an den Server; wobei der Server ferner Folgendes umfasst Mittel zum Erzeugen eines Sitzungsschlüssels, Mittel zum Verschlüsseln des Satzes von Zugangscodes mit dem Sitzungsschlüssel zum Erzeugen eines mit dem Sitzungsschlüssel verschlüsselten Satzes, Mittel zum Verschlüsseln des Sitzungsschlüssels mit dem öffentlichen Schlüssel zum Erzeugen eines mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels und Mittel zum Senden einer Nachricht, welche den mit dem Sitzungsschlüssel verschlüsselten Satz und den mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel enthält, über das Netz an das Benutzergerät; und bei welcher das Benutzergerät ferner Folgendes umfasst: Mittel zum Entschlüsseln des mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels mit dem privaten Schlüssel des Paars zum Wiederherstellen des Sitzungsschlüssels, Mittel zum Entschlüsseln des mit dem Sitzungsschlüssel verschlüsselten Satzes mit dem wiederhergestellten Sitzungsschlüssel zum Wiederherstellen des Satzes und Mittel zum Speichern des entschlüsselten Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

30. Einrichtung nach einem der Ansprüche 22 bis 29, bei welcher die Zugangscodes Einmal-Authentifizierungscodes sind.

31. Einrichtung nach einem der Ansprüche 22 bis 28, bei welcher das Netz ein drahtloses Datenübertragungsnetz umfasst.

32. Einrichtung nach Anspruch 31, bei welcher das Benutzergerät ein Mobiltelefon, einen persönlichen digitalen Assistenten oder eine Smartcard umfasst.

33. Einrichtung nach Anspruch 31, bei welcher die Nachrichten SMS-Nachrichten sind.

34. Benutzergerät zum Empfangen eines Satzes von Zugangscodes über ein Datenübertragungsnetz von einem Server, wobei das Benutzergerät Folgendes umfasst:
Mittel zum Speichern eines kryptografischen Schlüssels und eines Kennungscodes; Mittel zum Senden einer Nachricht, welche den Kennungscode enthält, über ein Datenübertragungsnetz an einen Server; Mittel zum Empfangen einer Nachricht, welche den Satz der mit dem Schlüssel verschlüsselten Zugangscodes enthält, vom Server; Mittel zum Entschlüsseln des empfangenen Satzes von Zugangscodes mittels des im Speicher gespeicherten Schlüssels; und Mittel zum Speichern des entschlüsselten Satzes von Zugangscodes zur Verwendung durch einen Benutzer des Benutzergerätes; und Mittel zum Empfangen einer Nachricht, welche einen mit dem neuen Schlüssel verschlüsselten Satz von Zugangscodes enthält, über das Netz vom Server nach dem

Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes.

35. Benutzergerät nach Anspruch 34, welches ferner Folgendes umfasst:
Mittel zum Entschlüsseln eines vom Server empfangenen neuen Schlüssels mittels des vorherigen Schlüssels; und Mittel zum Speichern des entschlüsselten neuen Schlüssels anstelle des vorherigen Schlüssels.

36. Benutzergerät nach Anspruch 35, welches ferner Folgendes umfasst:
Mittel zum Entschlüsseln des mit dem neuen Schlüssel verschlüsselten Satzes mittels des neuen Schlüssels; und Mittel zum Speichern des entschlüsselten neuen Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

37. Benutzergerät nach Anspruch 34, welches ferner Folgendes umfasst:
Mittel zum Erzeugen eines Paars öffentlicher/privater Schlüssel; Mittel zum Senden einer Nachricht, welche den öffentlichen Schlüssel des Paars enthält, über das Netz an den Server; Mittel zum Empfangen einer Nachricht, welche einen mit dem Sitzungsschlüssel verschlüsselten Satz von Zugangscodes und einen mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel enthält, über das Netz vom Server; Mittel zum Entschlüsseln des mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels mit dem privaten Schlüssel des Paars zum Wiederherstellen des Sitzungsschlüssels; Mittel zum Entschlüsseln des mit dem Sitzungsschlüssel verschlüsselten Satzes mit dem wiederhergestellten Sitzungsschlüssel zum Wiederherstellen des Satzes; und Mittel zum Speichern des entschlüsselten Satzes zur Verwendung durch einen Benutzer des Benutzergerätes.

38. Server zum Bereitstellen eines Satzes von Zugangscodes für ein Benutzergerät über ein Datenübertragungsnetz, wobei der Server Folgendes umfasst:
Mittel zum Speichern eines kryptografischen Schlüssels, welcher einem in dem Benutzergerät gespeicherten kryptografischen Schlüssel entspricht; Mittel zum Zuweisen des Satzes von Zugangscodes zum Benutzergerät nach dem Empfang einer Nachricht, welche einen Kennungscode enthält, über das Netz von dem Benutzergerät; Mittel zum Ausführen einer Suchfunktion anhand des in der Nachricht empfangenen Kennungscodes zum Abrufen des Schlüssels vom Speicher; Mittel zum Verschlüsseln des Satzes von Zugangscodes mittels des abgerufenen Schlüssels zum Erzeugen eines verschlüsselten Satzes; und Mittel zum Senden einer Nachricht, welche den verschlüsselten Satz enthält, über das Netz an das Benutzergerät, Mittel zum Senden einer Nachricht, welche den neuen Satz von Zugangscodes enthält, über das Netz an das Benutzergerät nach dem Erreichen eines vorgegebenen Schwellenwertes durch die Anzahl der unbenutzten Zugangscodes.

39. Server nach Anspruch 38, welcher ferner Folgendes umfasst:
Mittel zum Erzeugen eines neuen Schlüssels und zum Verschlüsseln des neuen Schlüssels mit dem vorherigen Schlüssel; und Mittel zum Senden einer Nachricht, welche den verschlüsselten neuen Schlüssel enthält, über das Netz an das Benutzergerät.

40. Server nach Anspruch 39, welcher ferner Folgendes umfasst:
Mittel zum verschlüsseln des neuen Satzes von Zugangscodes mit dem neuen Schlüssel zum Erzeugen eines mit dem neuen Schlüssel verschlüsselten Satzes.

41. Server nach Anspruch 38, welcher ferner Folgendes umfasst:
Mittel zum Empfangen einer Nachricht, welche einen öffentlichen Schlüssel eines Paars öffentlicher/privater Schlüssel enthält, vom Benutzergerät; Mittel zum Erzeugen eines Sitzungsschlüssels; Mittel zum Verschlüsseln des Satzes von Zugangscodes mit dem Sitzungsschlüssel zum Erzeugen eines mit dem Sitzungsschlüssel verschlüsselten Satzes; Mittel zum Verschlüsseln des Sitzungsschlüssels mit dem öffentlichen Schlüssel zum Erzeugen eines mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssels; und Mittel zum Senden einer Nachricht, welche den mit dem Sitzungsschlüssel verschlüsselten Satz und den mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel enthält, über das Netz an das Benutzergerät.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen

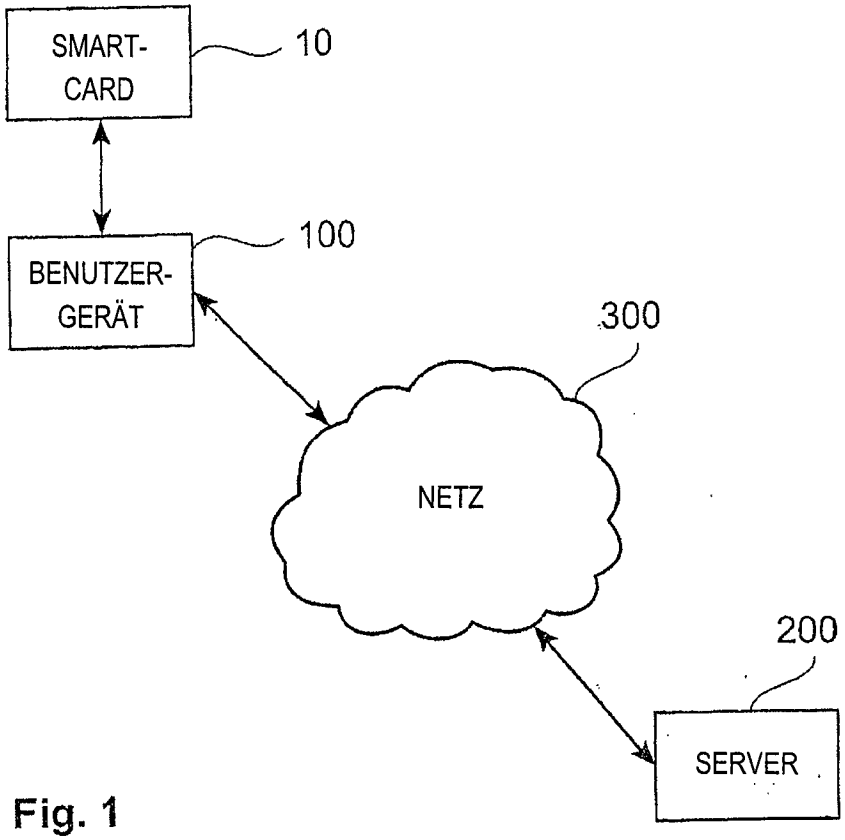

Fig. 1

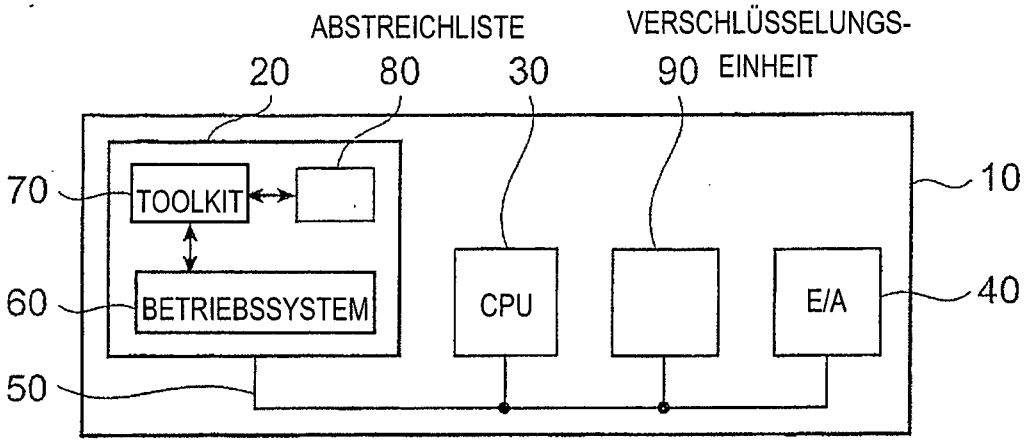

Fig. 2

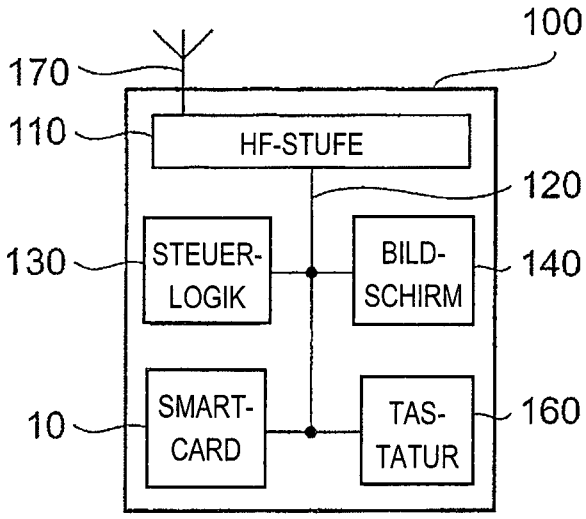

Fig. 3

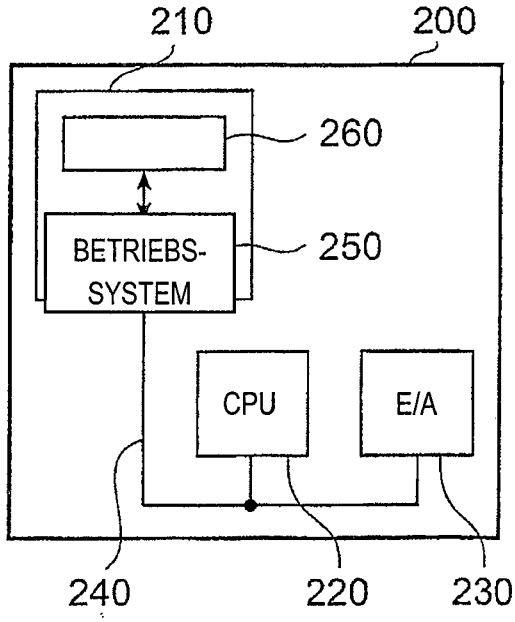

Fig. 4

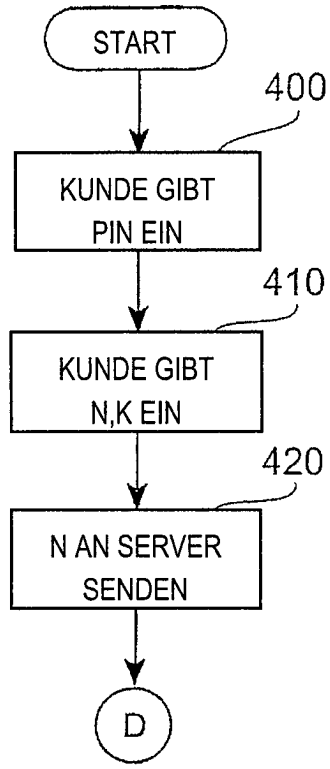

Fig. 5

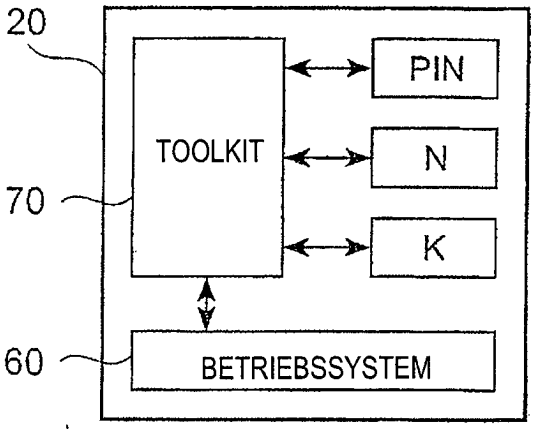

Fig. 6

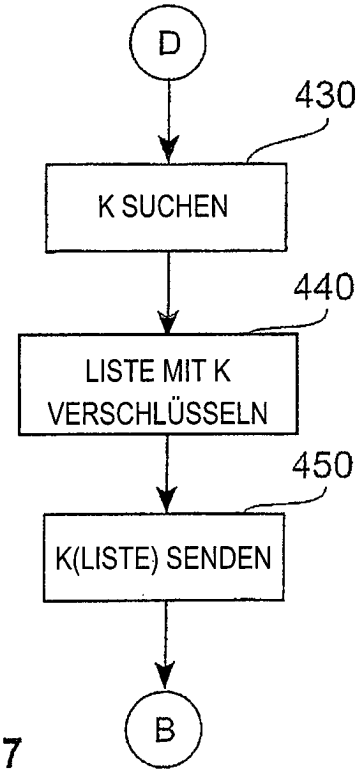

Fig. 7

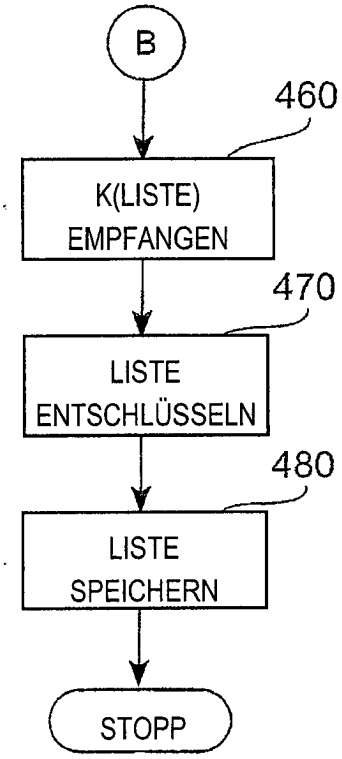

Fig. 8

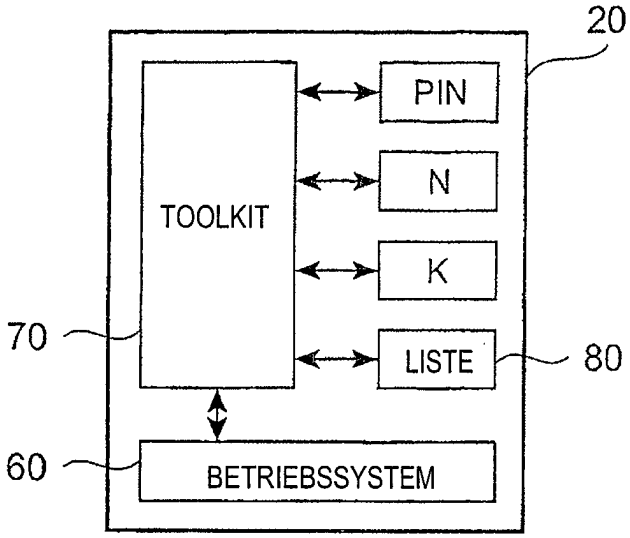

Fig. 9

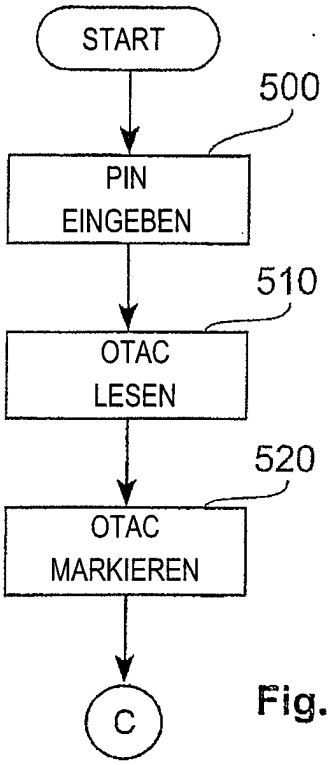

Fig. 10

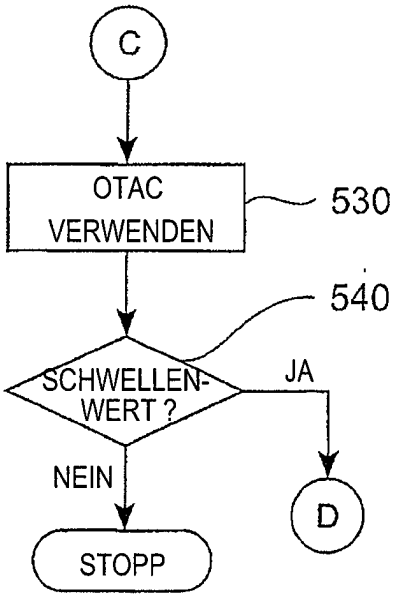

Fig. 11

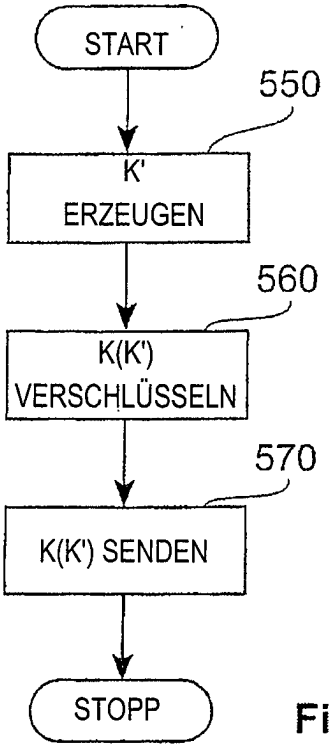

Fig. 12

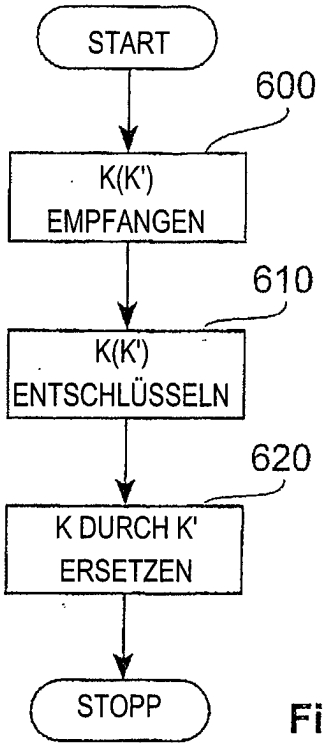

Fig. 13

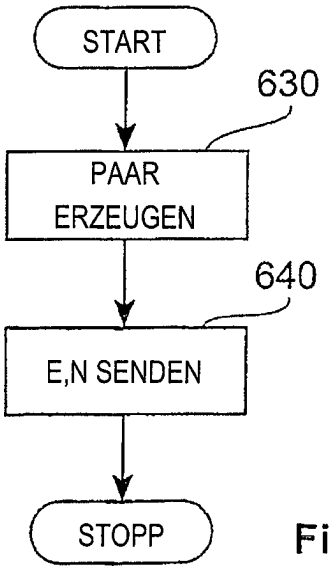

Fig. 14

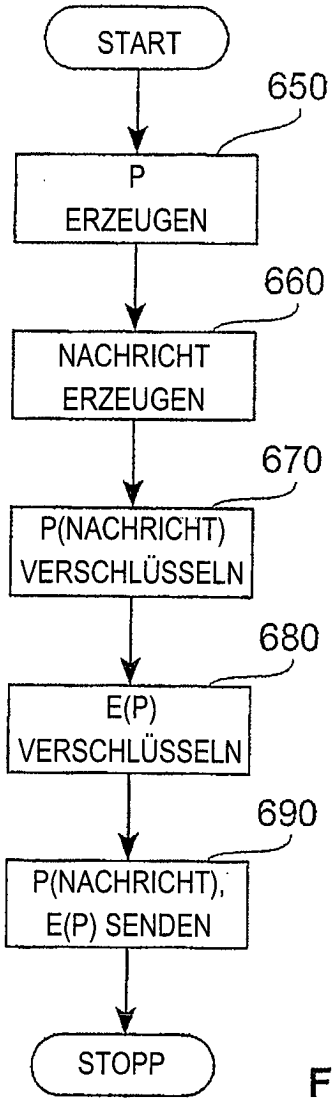
START
650
P
ERZEUGEN
660
NACHRICHT
ERZEUGEN
670
P(NACHRICHT)
VERSCHLÜSSELN
680
E(P)
VERSCHLÜSSELN
690
P(NACHRICHT),
E(P) SENDEN
STOPP

Fig. 15

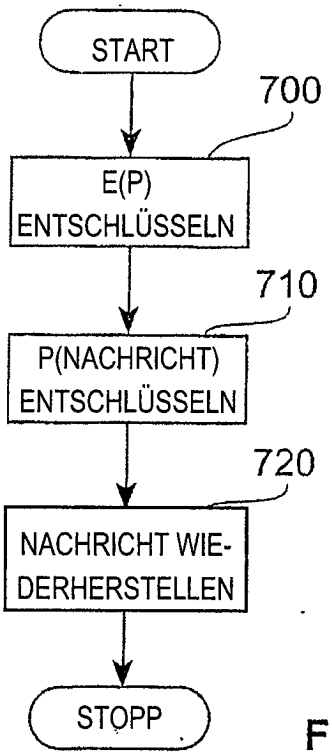
START
700
E(P)
ENTSCHLÜSSELN
710
P(NACHRICHT)
ENTSCHLÜSSELN
720
NACHRICHT WIE-
DERHERSTELLEN
STOPP

Fig. 16

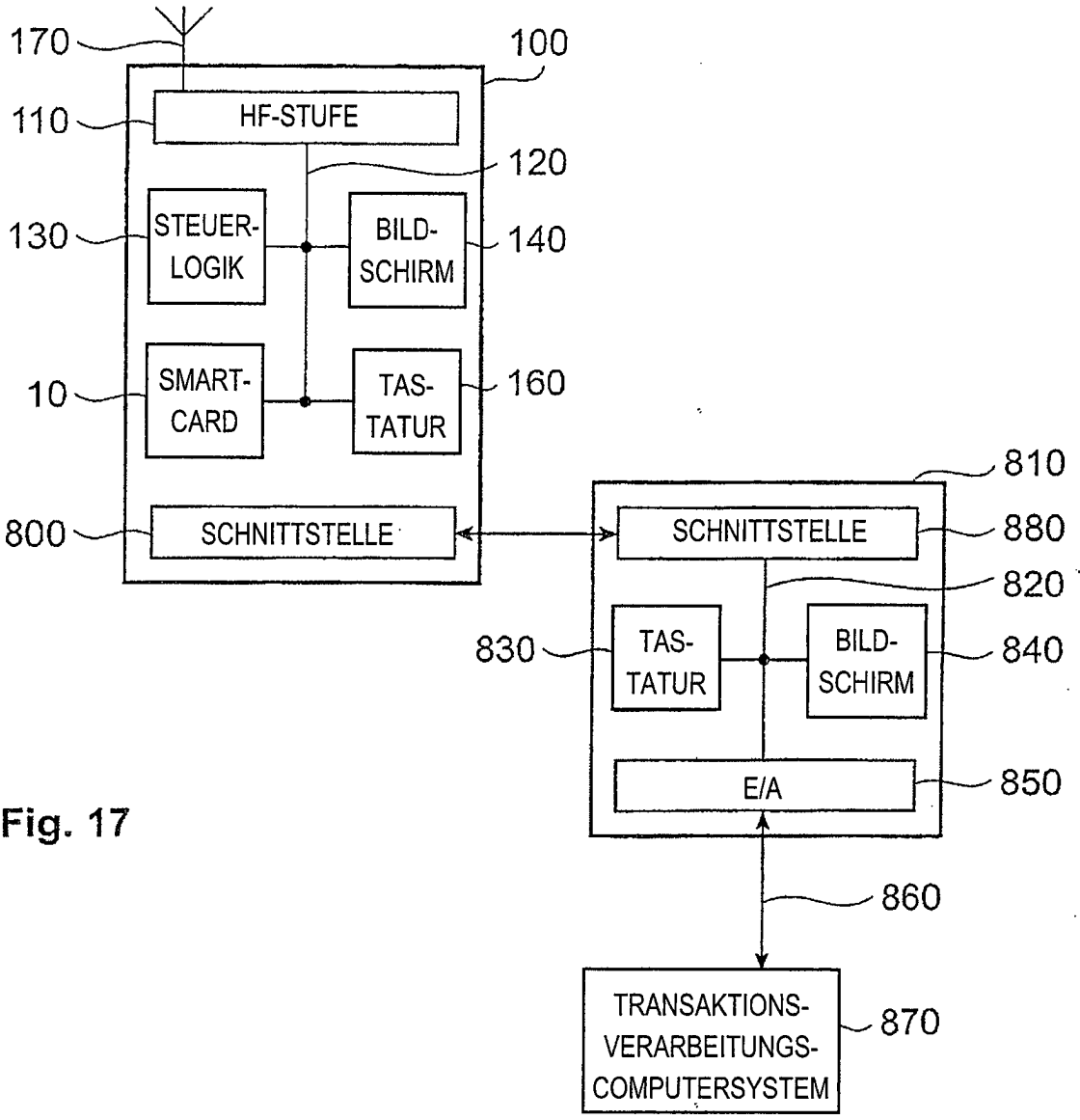
170
100
110
HF-STUFE
120
130
STEUER-LOGIK
BILD-SCHIRM
140
10
SMART-CARD
TAS-TATUR
160
800
SCHNITTSTELLE
810
SCHNITTSTELLE
880
820
830
TAS-TATUR
BILD-SCHIRM
840
E/A
850
860
TRANSAKTIONS-VERARBEITUNGS-COMPUTERSYSTEM
870

Fig. 17