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

(10) **DE 696 30 713 T2** 2004.12.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 912 959 B1**
(21) Deutsches Aktenzeichen: **696 30 713.8**
(86) PCT-Aktenzeichen: **PCT/US96/07185**
(96) Europäisches Aktenzeichen: **96 916 498.7**
(87) PCT-Veröffentlichungs-Nr.: **WO 96/036934**
(86) PCT-Anmeldetag: **17.05.1996**
(87) Veröffentlichungstag der PCT-Anmeldung: **21.11.1996**
(97) Erstveröffentlichung durch das EPA: **06.05.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **12.11.2003**
(47) Veröffentlichungstag im Patentblatt: **02.12.2004**

(51) Int Cl.[7]: **G06K 9/00**
G07C 9/00, G07F 7/10

(30) Unionspriorität:
442895 **17.05.1995** **US**

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

(73) Patentinhaber:
Indivos Corp., Oakland, Calif., US

(74) Vertreter:
LEINWEBER & ZIMMERMANN, 80331 München

(72) Erfinder:
HOFFMAN, Ned, Berkeley, US; PARE, F., David, Berkeley, US; LEE, A., Jonathan, Berkeley, US

(54) Bezeichnung: **IDENTIFIKATIONSSYSTEM OHNE IDENTITÄTSMARKER**

Beschreibung

[0001] Die Verwendung von Identitätsmarkern (Tokens) und Kreditkarten ist in der heutigen Finanzwelt allgemein üblich. Ein Token ist jedes leblose Objekt, das einem das Objekt präsentierenden Individuum bzw. Benutzer eine Fähigkeit verleiht. Fernzugriff auf jedes beliebige Finanzkonto erfolgt z. B. mittels des Einsatzes von Tokens oder Plastikkarten. Ob man nun Lebensmittel mit Kontokarten oder Verbrauchsgüter mit Kreditkarten bezahlt – der jeweiligen Finanztransaktion liegt eine durch einen Token aktivierte Geldüberweisung zugrunde, wobei der Token ein Individuum und das Finanzkonto, auf das er oder sie zugreift, identifiziert.

[0002] Der Grund für den Umstieg von Metallmünzen auf Plastikkarten ist ein einfacher: Der Zugriff auf Geld in diesem Geldüberweisungssystem ist sowohl für die Händler als auch für die Verbraucher ungleich sicherer und bequemer, als wenn man mit großen Mengen an Münzen und Banknoten hantieren müsste.

[0003] Leider ist die aktuelle Technologie in Kombination mit diesem bequemen Token-basierten Geldüberweisungssystem diebstahls- und betrugsanfällig.

[0004] Da die Verifizierung der Benutzeridentität lediglich auf den auf dem Token abgespeicherten Daten basiert, die leicht reproduzierbar und zwischen Individuen übertragen werden können, ist ein derartiges Sicherheitssystem notgedrungen auf den Fleiß und auch das Glück des autorisierten Benutzers und Händlers angewiesen, die diese Information als proprietär aufrechterhalten müssen. Es liegt aber in der Natur von Tokens, dass sie keine besonders ausgeprägte Beziehung zum Individuum haben. Die Identizierung des rechtmäßigen Besitzers des Tokens durch den Token ist bestenfalls aufwendig. Dies wird leicht durch die Tatsache veranschaulicht, dass andere Personen als die rechtmäßigen Besitzer der Tokens diese dazu benutzt haben, um Betrug an Händlern und anderen Verkäufern von Konsumgütern zu begehen.

[0005] Die ungeheure Expansion der Verbraucherkreditindustrie in den achtziger Jahren brachte hohe Gewinne für Kreditgeber und auch viele praktische Vorteile für Konsumenten mit sich. Je leichter es jedoch für Konsumenten wurde, einen Verbraucherkredit aufzunehmen, desto mehr wurden diese Kredite auch zur Zielscheibe von Kriminellen. So wie die durch das Automobil gesteigerte Mobilität zu einer Welle an Banküberfällen in den späten zwanziger Jahren und frühen dreißiger Jahren des 20. Jahrhunderts führte, so ergeben sich aufgrund des Überhandnehmens von Verbraucherkrediten immer mehr Möglichkeiten für illegale Geschäfte.

[0006] Die Bankenbranche war bereit, Verluste infolge von Betrug bis zu einem gewissen Grad zu akzeptieren, und wälzte die Kosten auf die Verbraucher ab. Je besser sich jedoch Kriminelle zu organisieren begannen, je technisch geschickter sie wurden und je mehr Personen im Handel arbeiten, die im Bereich Kreditkartensicherheit nur über mangelhafte Kenntnisse verfügen, desto sprunghafter stiegen die auf Betrug zurückzuführende Verluste an. Die dramatischen Statistiken über Betrugsfälle und durch Präventivmaßnahmen entstandene Kosten zwangen insbesondere die Kreditkartenfirmen dazu, sich nach anderen Problemlösungen umzusehen.

[0007] Auf Betrugsfälle zurückzuführende Verluste in der Kreditkartenindustrie haben aufgrund der hohen Anfälligkeit des Systems verschiedene Ursachen, doch am häufigsten kommt es durch verlorene, gestohlene oder gefälschte Karten zu solchen Verlusten. Kreditkarten sind nicht mit einem persönlichen Identifizierungscode (PIC) versehen, weshalb eine verlorene Kreditkarte in Bargeld umgemünzt werden kann, wenn sie in die falschen Hände gerät. Während Diebstahl eines Tokens noch immer der häufigste Grund für Systembetrug darstellt, ist auch die Verwendung gefälschter Kreditkarten ein immer größeres Problem. Gefälschte Kreditkarten werden von technisch versierten Kriminellen hergestellt, die an die gültige Kontonummer des Karteninhabers gelangen und dann unter Verwendung dieser gültigen Nummer eine gefälschte Karte produzieren. Der Fälscher kodiert den Magnetstreifen und prägt die gefälschte Plastikkarte mit der Kontonummer. Die Karte wird dann den Vertragspartnern in den Geschäften vorgelegt und das Konto des Karteninhabers entsprechend belastet. Eine weitere Form von Verlust ist die betrügerische und heimliche Ermittlung der Kontonummer des Karteninhabers durch den Kreditkarten-Vertragspartner. Eine weitere Art des Betrugs liegt vor, wenn der autorisierte Karteninhaber den Token für Einkäufe verwendet und nachher behauptet, der Token wäre gestohlen worden oder verloren gegangen. Man schätzt, dass Verluste aufgrund aller dieser Betrügereien pro Jahr mehr als 950 Millionen Dollar ausmachen.

[0008] Im Allgemeinen sind Kontokarten mit einem persönlichen Identifizierungscode (PIC) versehen. Das Fälschen einer Kontokarte ist komplizierter, da der Kriminelle nicht nur die Kontonummer, sondern auch den PIC in Erfahrung bringen und die Karte dann wie im obigen Kreditkarten-Beispiel herstellen muss. Es wurden aber bislang verschiedene Strategien entwickelt, um PICs von unvorsichtigen Karteninhabern zu erlangen.

Dies reicht von Geldausgabeautomaten in Einkaufszentren mit der Funktion eines eingebauten Trojanischen Pferds, die Bargeld ausgeben, aber den PIC aufzeichnen, über Vorrichtungen in Geschäften, die auch den PIC aufzeichnen, bis hin zu Personen mit Ferngläsern, die Karteninhaber bei der Eingabe ihrer PICs an den Geldausgabeautomaten beobachten. Die anschließend produzierten gefälschten Kontokarten werden dann in verschiedenen Geldausgabeautomaten ausprobiert, bis das Konto des unglücklichen Karteninhabers geleert ist.

[0009] Die Finanzindustrie ist sich des Kostenanstiegs durch Betrugsfälle bewusst und ergreift ständig Maßnahmen, um die Kartensicherheit zu verbessern. Somit haben Betrug und Diebstahl von Tokens einen indirekten Einfluss auf die Kosten des gesamten Systems.

[0010] Kartenrohlinge werden unter Einhaltung strenger Sicherheitsvorschriften erzeugt. Dann werden sie mit der Kontonummer und dem Ablaufdatum individualisiert und dem Karteninhaber zugeschickt. Die Produktion und der Vertrieb der Karten alleine kostet die Branche eine geschätzte Milliarde Dollar jährlich. Eine Standardkarte kostet die Finanzindustrie jeweils 2 Dollar, doch nur 0,30 Dollar davon entfallen auf tatsächliche Fertigungsschritte.

[0011] Im Laufe der letzten 10 Jahre hat die Industrie begonnen, die Tokens aufgrund der überhand nehmenden Fälschungen zu verändern, ohne dass sich die Nutzungsgewohnheiten des Kredittransaktionssystems nachhaltig verändert hätten. Man schaffte vor allem durch administrative Veränderungen Abhilfe – z. B. dass Kunden den Aussteller anrufen müsse, um ihre Karte zu aktivieren. Andere Veränderungen betrafen neue Elemente (Hologramme, Lichtbilder) oder Verbesserungen im Unterschriftsfeld. Vor allem diese Veränderungen sind ein Anzeichen dafür, dass die Betrugsanfälligkeit der Systeme auf einen Mangel an echter Identifizierungsmöglichkeit des Individuums zurückzuführen ist. Man schätzt, dass dies die Herstellungskosten auf zwei Milliarden Dollar jährlich, d. h. auf das Doppelte, ansteigen lassen könnte.

[0012] In der absehbaren Zukunft kann man davon ausgehen, dass im Bankenbereich eine noch teurere Karte, die so genannte „Smart Card", eingeführt wird. Smart Cards enthalten so viel Computerleistung wie einige der ersten PCs. Aktuelle Kostenschätzungen für Smart Cards der ersten Generation gehen von etwa $ 3,50 (ausschließlich der Vertriebskosten) aus, was deutlich höher als die $ 0,30 für Plastikkartenrohlinge ist.

[0013] Der signifikante Kostenanstieg zwang die Industrie dazu, neue Möglichkeiten auszuloten, um die Leistungsfähigkeit der Smart Cards zusätzlich zu der simplen Transaktionsautorisierung zu nutzen. Man denkt daran, dass auf Smart Cards neben den Kredit- und Girokontonummern auch Telefonnummern, Vielfliegermeilen, Geschäftsgutscheine, Daten zu früheren Transaktionen, Daten betreffend die elektrische Geldbörse (für Mautstationen und in öffentlichen Verkehrssystemen von Belang) sowie der Namen des Kunden, lebensnotwendige Statistiken und vielleicht sogar medizinische Informationen gespeichert sind. Klarerweise möchte man in der Finanzindustrie die weitere Verbreitung von Tokens forcieren.

[0014] Die Nebenwirkung der verbesserten Leistungen von Smart Cards ist die Zentralisierung von Funktionen. Anders ausgedrückt: Der Preis, den man für ein Mehr an Funktionalität zahlen muss, ist höhere „Verwundbarkeit". Aufgrund der Anzahl an Funktionen, die man mithilfe einer Smart Card erfüllen kann, wäre ein Verlust oder eine Beschädigung einer solchen „Monsterkarte" für den Karteninhaber äußerst unangenehm. Keine derartige Karte zu besitzen bedeutet für den Karteninhaber, dass er finanziell handlungsunfähig ist, bis die Karte ersetzt wurde. Außerdem führt ein Verlust einer Karte mit prall gefüllter elektronischer Geldbörse auch zu einem realen finanziellen Verlust. Weiters hat man sich noch nicht überlegt, inwieweit Fälscher eines Tages in der Lage sein werden, eine Smart Card zu kopieren.

[0015] Aufgrund der geplanten Konzentration von Funktionen auf der Smart Card sind Karteninhaber Verlusten oder Beschädigungen der Karte schutzloser ausgeliefert als davor. Nach der Investition riesiger Geldmengen wird demnach das daraus resultierende System einen höheren Grad an Sicherheit aufweisen, doch der Preis, den die Konsumenten für den Verlust oder die Beschädigung von Smart Cards zu zahlen haben, wird immer höher sein.

[0016] Die Finanzindustrie ist sich der mit Smart Cards verbundenen Sicherheitsbedenken bewusst, und es werden derzeit auch Anstrengungen unternommen, die Fälschung von Plastikkarten entsprechend zu erschweren. Milliarden von Dollars werden in den nächsten fünf Jahren in Projekte fließen, Kreditkarten noch sicherer zu machen.

[0017] Bislang war die Kreditkartenindustrie mit einer einfachen Gleichung konfrontiert: Um Betrug hintanzuhalten, müssen die Kartenkosten gesteigert werden.

[0018] Neben der allgemeinen Verbreitung von elektronischen Transaktionen sind auch elektronische Faxübertragungen, E-Mail-Systeme und ähnliche elektronische Kommunikationstechnologien gang und gäbe. Ein Problem, das der mangelnden Identifizierungsmöglichkeit von Individuen bei finanziellen Transaktionen ähnelt, ist die mangelnde Identifizierungsmöglichkeit von Individuen bei elektronischen Übertragungen. Die Leichtigkeit und die Geschwindigkeit elektronischer Kommunikation und ihre niedrigen Kosten im Vergleich zur konventionellen Post machen sie zu einem bevorzugten Kommunikationsmedium im privaten und im geschäftlichen Bereich. Diese Art der Kommunikation ist in letzter Zeit stark angestiegen, und diese Expansion wird sich vermutlich auch fortsetzen. Doch Millionen elektronischer Nachrichten wie z. B. Faxe und E-Mails werden versendet, ohne zu wissen, ob sie an ihrem richtigen Bestimmungsort ankommen oder ob eine bestimmte Person sie tatsächlich verschickt oder empfangen hat. Außerdem kann man die Person nicht kontrollieren, die eine elektronische Nachricht versendete oder empfing.

[0019] In letzter Zeit wurden verschiedene Versuche unternommen, Probleme in Zusammenhang mit Token- und Codesicherheitssystemen zu lösen. Man konzentrierte sich u. a. darauf, den PIC zu verschlüsseln, zu variabilisieren oder in anderer Weise zu modifizieren, um es einem nicht autorisierten Benutzer zu erschweren, mehr als eine Transaktion durchzuführen; dabei versucht man, den PIC so zu manipulieren, dass er betrugssicherer wird. Es wurden in diesem zahlreiche Methoden vorgeschlagen, z. B. die Einführung eines Algorithmus, der den PIC in einer vorhersagbaren Weise, die nur dem Benutzer bekannt ist, variiert, wobei für jeden nachfolgenden Zugriff auf ein Konto ein anderer PIC notwendig ist. Der PIC kann z. B. variiert und für jeden Kalendertag bzw. für jedes Datum des versuchten Zugriffs spezifiziert werden. Ein anderes Verfahren sieht die Einführung eines zeitvariablen Elements vor, um einen nicht vorhersagbaren PIC zu generieren, der nur einem autorisierten Benutzer zum Zeitpunkt des Zugriffs präsentiert wird. Obwohl solche Systeme betrugssicherer sind als Systeme mit nichtvariablen Codes, ist ein derartiges System auch nicht vollkommen betrugssicher, da es nach wie vor mit Daten operiert, die nicht eindeutig und unwiderlegbar auf den autorisierten Benutzer zutreffen. Außerdem bedeuten solche Systeme für Benutzer, die ohnedies mit dem Merken konstanter Codes – geschweige denn variabler Codes – Schwierigkeiten haben, zusätzliche Probleme. Beispiele für Verfahren dieser Art sind in den US-Patenten 4.837.422 (Dethloff et al.), 4.998.279 (Weiss), 5.168.520 (Weiss), 5.251.259 (Mosley), 5.239.538 (Parrillo), 5.276.314 (Martino et al.) und 5.343.529 (Goldfine et al.) geoffenbart.

[0020] In letzter Zeit schenkte man nicht nur PICs, sondern auch eindeutiger Biometrik als Basis der Verifikation von Identität und letzten Endes auch als Basis des Computerzugriffs mehr Aufmerksamkeit. Dabei werden authentifizierte biometrische Daten eines Benutzers bekannter Identität aufgezeichnet und für zukünftige Kontrollen auf einem Token gespeichert. Bei jedem nachfolgenden versuchten Zugriff muss der Benutzer die angeforderten biometrischen Daten eingeben, die dann mit den authentifizierten biometrischen Daten auf dem Token verglichen werden, um zwecks Verifizierung der Benutzeridentität zu bestimmen, ob die beiden übereinstimmen. Da die biometrischen Daten eindeutig auf den Benutzer zutreffen und da die Tätigkeit der physischen Eingabe biometrischer Daten praktisch nicht zu reproduzieren ist, bedeutet Übereinstimmung vermutlich auch Vorliegen der richtigen Identität, was das Betrugsrisiko mindert. Es wurden verschiedene biometrische Daten vorgeschlagen, z. B. Fingerabdrücke, Handabdrücke, Stimmabdrücke, Netzhautbilder, Unterschriftsproben u. dgl. Da jedoch die biometrischen Daten im Allgemeinen in elektronischer – und somit reproduzierbarer – Weise auf einem Token gespeichert werden und das Abgleichs- und Verifizierungsverfahren nicht isoliert von der Hardware und Software abläuft, die direkt von der den Zugriff versuchenden Person verwendet wird, besteht aber noch immer ein signifikantes Risiko, dass betrügerischer Zugriff vorliegt. Beispiele für diese Systeme sind in folgenden US-Patenten geoffenbart: 4.821.118 (Lafreniere), 4.993.068 (Piosenka et al.), 4.995.086 (Lilley et al.), 5.054.089 (Uchida et al.), 5.095.194 (Barbanell), 5.109.427 (Yang), 5.109.428 (Igaki et al.), 5.144.680 (Kobayashi et al.), 5.146.102 (Higuchi et al.), 5.180.901 (Hiramatsu), 5.210.588 (Lee), 5.210.797 (Usui et al.), 5.222.152 (Fishbine et al.), 5.230.025 (Fishbine et al.), 5.241.606 (Horie), 5.265.162 (Bush et al.), 5.321.242 (Heath, Jr.), 5.325.442 (Knapp) und 5.251.303 (Willmore).

[0021] Es ergibt sich aus den obigen Ausführungen, dass zwischen dem Versuch, ein Sicherheitssystem zu entwickeln, das äußerst betrugssicher, aber trotzdem leicht und praktisch in der Anwendung ist, eine dynamische – und unvermeidliche – Spannung besteht. Keine der oben geoffenbarten Verbesserungen des Token- und Codesystems wird dieser Spannung gerecht bzw. kann sie mindern. Solche Systeme speichern im Allgemeinen authentifizierte biometrische Daten in elektronischer Form direkt auf dem Token, die vermutlich kopiert werden können. Außerdem schützen solche Systeme den Identifizierungs-Verifizierungsvorgang nicht ausreichend vor unerlaubten Eingriffen von Personen.

[0022] Ein Beispiel eines Sicherheitssystems auf Token-Basis, das mit biometrischen Daten eines Benutzers operiert, ist in US-Patent 5.280.527 (Gullman et al.) geoffenbart. In dieser Patentveröffentlichung muss der Benutzer einen Token in Kreditkartengröße (als biometrische Sicherheitsvorrichtung bezeichnet) tragen, in dem

ein Mikrochip enthalten ist, auf dem Eigenschaften der Stimme des autorisierten Benutzers gespeichert sind. Um die Zugriffsprozedur einzuleiten, muss der Benutzer den Token in ein Endgerät wie z. B. einen Geldausgabeautomat einschieben und dann mit diesem sprechen, um eine biometrische Eingabe vorzunehmen, die dann mit einer auf dem Mikrochip des präsentierten Tokens gespeicherten authentifizierten Eingabe verglichen wird. Das Verfahren der Identitätsverifizierung ist im Allgemeinen nicht vor potenziellen unerlaubten bzw. unautorisierten Eingriffen geschützt. Wenn eine Übereinstimmung festgestellt wird, kann dann das Fern-Endgerät dem Hostcomputer signalisieren, dass Zugriff gestattet werden sollte, oder den Benutzer auffordern, einen zusätzlichen Code wie z. B. einen PIN (auch auf dem Token abgespeichert) einzugeben, bevor das notwendige Verifizierungssignal an den Hostcomputer geschickt wird.

[0023] Dieses Patent beruht auf dem Vergleich gespeicherter und eingegebener biometrischer Daten, wodurch das Risiko des unerlaubten Zugriffs im Vergleich zu numerischen Codes reduziert wird; trotzdem machen Gullmanns Verwendung des Tokens als Speicherort von Authentifizierungsdaten sowie die Unmöglichkeit, den Prozess der Identitätsverifizierung vor unerlaubten Eingriffen zu schützen, die Verbesserungen der Betrugssicherheit, die sich durch den Wechsel von einem numerischen Code zur Biometrik ergeben, zunichte. Außerdem bleibt das System in der Verwendung etwas kompliziert und unpraktisch, da es auch die Präsentation eines Tokens erfordert, um eine Zugriffsaufforderung einzuleiten.

[0024] Patente, die Token-basierte Systeme offenbaren, lehren fast nie die biometrische Erkennung ohne die Verwendung von Tokens. Die angeführten Gründe dafür sind die Speicheranforderungen für biometrische Erkennungssysteme sowie lange Zeiträume zur Identifizierung einer großen Anzahl an Individuen (selbst für die leistungsstärksten Computer).

[0025] Die US-5.335.288 offenbart ein Token-loses biometrisches Erkennungssystem, das ein Silhouettenbild der Hand eines Benutzers speichert. Dieses Bild wird mit einem Bild verglichen, das in einem nachfolgenden Bid-Vorgang erhalten wird, um die Benutzeridentität entweder zu verifizieren oder zu ermitteln. Im Verifizierungssystem ist jedem Bild ein PIN-Code zugeordnet, und während eines nachfolgenden Bid-Vorgangs gibt ein Benutzer den Code ein, präsentiert seine Hand zwecks Bildgebung, und dann wird überprüft, ob das Handbild und der PIN-Code mit den gespeicherten übereinstimmen. Im Identifizierungssystem präsentiert der Benutzer nur seine Hand zwecks Bildgebung, und dann erfolgt eine Suche unter den gespeicherten Bildern, um den Benutzer zu identifizieren. Die gespeicherten Bilder können auf der Basis eines Handmerkmals in einem Teilsatz gruppiert werden.

[0026] Angesichts der obigen Ausführungen ist offensichtlich, dass die Notwendigkeit besteht, ein Computerzugriffssystem zu entwickeln, das äußerst betrugssicher, praktisch und effizient in der Bedienung ist, um elektronische Transaktionen und Übertragungen zügig durchführen zu können.

[0027] Es besteht ferner die Notwendigkeit, ein Computersystem zu entwickeln, das vollkommen ohne Token funktioniert und die persönliche Identität eines Benutzers lediglich auf der Basis eines persönlichen Identifizierungscodes und biometrischer Daten verifizieren kann, die eindeutig und physisch dem autorisierten Benutzer zuordenbar sind, anstelle der Kontrolle, ob ein Individuum ein physisches Objekt besitzt, das leicht auf andere Personen übertragbar ist. Solche biometrischen Daten müssen leicht und ohne großen Aufwand erhalten werden können; sie müssen einfach und kostengünstig zu speichern und zu analysieren sein; und sie dürfen das Recht des Benutzers auf Privatsphäre nicht über Gebühr einschränken.

[0028] Ein weiterer Faktor bei der Konstruktion von Computerzugriffssystemen ist die Benutzerfreundlichkeit. Es ist äußerst wünschenswert, dass ein Konsument spontan und mit minimalem Aufwand auf das System zugreifen kann, insbesondere wenn sich eine Notfallssituation einstellt. Insbesondere ist es notwendig, dass es das System überflüssig macht, sich zahlreiche komplizierte Codes zu merken oder ein proprietäres Objekt zu besitzen, mit sich zu tragen und vorzulegen, um eine Zugriffsaufforderung einzuleiten.

[0029] Solche Systeme müssen einfach in der Bedienung, präzise und zuverlässig sein. Außerdem ist ein Computerzugriffssystem erforderlich, das den Zugriff von Benutzern auf mehrere Konten ermöglicht, alle dem Benutzer zur Verfügung stehende Dienste anbietet und Transaktionen in und zwischen allen Finanzkonten durchführt, Zahlungen in den Geschäftslokalen vornimmt, verschiedene Dienste empfängt usw.

[0030] Außerdem ist ein Computerzugriffssystem notwendig, das einem autorisierten Benutzer die Möglichkeit gibt, Behörden davon in Kenntnis zu setzen, dass ein Dritter den Benutzer zur Zugriffsaufforderung zwingt, ohne dass dieser Dritte erfährt, dass ein Alarm aktiviert wurde. Ein derartiges System soll auch trotzdem in der Lage sein, ohne das Wissen des den Benutzer zur Aufforderung zwingenden Dritten vorübergehend die Art

und den Umfang von Transaktionen einzuschränken, die – sobald der Zugriff erlaubt ist – durchgeführt werden können.

[0031] Außerdem muss das Computersystem kostengünstig und flexibel genug sein, um kompatibel mit existierenden Netzwerken betrieben zu werden, die eine Vielzahl elektronischer Transaktions- und Übertragungsvorrichtungen und Systemkonfigurationen aufweisen.

[0032] Schließlich besteht die Notwendigkeit des sicheren Verschickens und Erhaltens von elektronischen Nachrichten und Faxen, wobei der Inhalt der elektronischen Nachricht vor der Offenbarung gegenüber unautorisierten Personen geschützt ist und die Identität des Senders oder Empfängers mit einem hohen Grad an Zuverlässigkeit ermittelt werden kann.

Zusammenfassung der Erfindung

[0033] Die vorliegende Erfindung erfüllt die oben angeführten Kriterien und stellt ein verbessertes Identifizierungssystem zur Bestimmung der Identität eines Individuums bzw. Benutzers bereit; es basiert auf einem Vergleich der biometrischen Probe und des persönlichen Identifizierungscodes des Individuums, die während eines Bid-Schritts erfasst wurden, mit der biometrischen Probe und dem persönlichen Identifizierungscode dieses Individuums, die während eines Registrierungsschritts erfasst und an einem entfernten Ort gespeichert wurden, an dem sich ein Datenverarbeitungszentrum befindet. Die Erfindung betrifft ein Computernetzwerk-Hostsystem mit Mitteln zum Vergleich der eingegebenen biometrischen Probe und des persönlichen Identifizierungscodes, ausgestattet mit verschiedenen Datenbanken und Speichermodulen. Außerdem umfasst die Erfindung eine biometrische und PIC-Eingabevorrichtung und Endgeräte zur Eingabe von Daten, um Informationen für die Ausführung der aufgeforderten Transaktionen und Übertragungen durch das Hostsystem bereitzustellen, sobald die Identität des Individuums bestimmt ist. Die Erfindung betrifft auch Mittel zur Verbindung des Hostsystems mit dem Endgerät und der biometrischen Eingabevorrichtung.

[0034] Der Computer besitzt auch Mittel zur Ausführung verschiedener Transaktionen und Übertragungen zusätzlich zur traditionellen Speicherung und Modifikation von Daten. Ferner kann der Computer die Bewertung des Biometrik-PIC-Vergleichs („persönlicher Identifizierungscode") und die Bestimmung einer Identifizierungsevaluierung bzw. den Exekutionsstatus jeder Transaktion oder Übertragung ausgeben. Darüber hinaus benachrichtigt oder authentifiziert das Computersystem das identifizierte Individuum, dass ein Zugriff auf das Computersystem erfolgte, indem dem Individuum ein privater Code zurückgeschickt wird, der zuvor während des Registrierungsschritts von diesem Individuum ausgewählt wurde.

[0035] Vorzugsweise ist das Computersystem vor elektronischem Abhören, elektronischem Eindringen und Viren geschützt. Außerdem würden die vom Computer zur Erfassung biometrischer Proben und persönlicher Identifizierungscodes verwendeten Vorrichtungen das Folgende umfassen: a) zumindest eine biometrische Eingabevorrichtung zur Erfassung biometrischer Proben, die über eine Hardware- und eine Softwarekomponente verfügt; b) zumindest ein Endgerät, das funktionell entweder teilweise oder zur Gänze mit der biometrischen Eingabevorrichtung integriert ist, um Zusatzinformationen einzugeben und anzufügen; c) zumindest ein Dateneingabegerät für die Eingabe eines persönlichen Identifizierungscodes, wobei dieses Dateneingabegerät entweder mit der biometrischen Eingabevorrichtung oder mit dem Endgerät integriert ist; und d) ein Mittel zur Zusammenschaltung der biometrischen Eingabevorrichtung, des Dateneingabegeräts und des Endgeräts. Das Endgerät besitzt auch zumindest eine Anzeige zur Anzeige von Daten und Informationen. Um zusätzliche Sicherheit zu bieten, identifiziert das Computersystem die biometrische Eingabevorrichtung sowie den Gegenteilnehmer oder den Vertragspartner (Händler) durch einen Gegenteilnehmer- oder Vertragspartner-Code, der mit dem Endgerät in Zusammenhang steht, der mit der biometrischen Eingabevorrichtung verbunden ist. Es ist auch zu bevorzugen, dass die biometrische Eingabevorrichtung vor unerlaubtem physischem und elektronischem Eingriff geschützt ist und dass im Fall des Bruchs der Vorrichtung Mittel zur physischen und/oder elektronischen Zerstörung von Komponenten innerhalb der Vorrichtung und/oder zum Löschen kritischer Daten aus den Speichermodulen der Vorrichtung eingesetzt werden.

[0036] Außerdem würde die biometrische Eingabevorrichtung eine Hardwarekomponente enthalten, die Folgendes umfasst: a) zumindest ein Berechnungsmodul zur Datenverarbeitung; b) löschbare und nicht löschbare Speichermodule zur Speicherung von Daten und Software; c) eine biometrische Abtastvorrichtung zur Eingabe von Biometrikdaten; d) Dateneingabemittel zum Eingeben von Daten; e) einen digitalen Kommunikationsanschluss; und f) eine Vorrichtung zur Verhinderung von elektronischem Abhören.

[0037] Um die Integrität und Vertraulichkeit elektronischer Daten zu schützen, die zwischen der biometrischen

Eingabevorrichtung, dem Endgerät und dem Computernetz versendet werden, ist es vorzuziehen, dass die Daten verschlüsselt und versiegelt sind.

[0038] Das Hostcomputernetzwerk ist durch herkömmliche Mittel auch mit anderen unabhängigen Computersystemen, Datenbanken, Faxgeräten und anderen Computernetzwerken verbunden und kann mit ihnen kommunizieren.

[0039] Das Verfahren der Erfindung umfasst das freiwillige Identifizieren eines Individuums ohne Verwendung eines Tokens mittels Überprüfung zumindest einer biometrischen Probe und eines persönlichen Identifizierungscodes, die dieses Individuum bereitstellt. Während eines Registrierungsschritts muss sich das Individuum im System mittels einer authentifizierten biometrischen Probe, eines persönlichen Identifizierungscodes und eines privaten Codes registrieren. Anschließend werden während eines Bid-Schritts die biometrische Probe und der persönliche Identifizierungscode des Individuums erfasst und mit jenen verglichen, die während des Registrierungsschritts registriert wurden. Eine Übereinstimmung des persönlichen Identifizierungscodes und der biometrischen Probe führt zur positiven Identifizierung des Individuums. Um dem identifizierten Individuum zu bestätigen, dass auf das reale Computersystem zugegriffen wurde, wird der private Code des Individuums, der im Registrierungsschritt erfasst wurde, an das Individuum zurückgeschickt.

[0040] Es ist vorzuziehen, dass das Verfahren der Erfindung ein Verfahren zur Untersuchung der biometrischen Proben während der Registrierung und während des Vergleichs solcher biometrischer Proben mit einer Sammlung biometrischer Proben von Individuen enthält, die als jene identifiziert wurden, die zuvor versucht haben, in betrügerischer Absicht in das System einzudringen oder tatsächlich bereits betrügerische Handlungen im System durchgeführt haben.

[0041] In einer bevorzugten Ausführungsform enthält die Erfindung ein Verfahren zur Benachrichtigung von Behörden, dass außergewöhnliche Umstände vorliegen oder dass der Benutzer unter Zwang steht.

[0042] Es ist auch bevorzugt, dass ein Verfahren zur Verschlüsselung und Versiegelung von Daten dazu herangezogen wird, die Daten einschließlich der digitalisierten biometrischen Probe davor zu schützen, irrtümlich oder mit krimineller Absicht während der Übertragung offenbart zu werden.

[0043] Es ist außerdem bevorzugt, dass das Verfahren Schritte vorsieht, die das Individuum setzen kann, um verschiedene Finanzkonten und verschiedene Arten elektronischer Übertragungen auszuwählen.

[0044] Ferner ist es bevorzugt, dass das Verfahren ein Verfahren zur Archivierung von Daten und elektronischen Übertragungen sowie zum Abrufen der archivierten Daten mittels eines Verfolgungscodes enthält.

[0045] Darüber hinaus ist es vorzuziehen, dass jedes Dokument, z. B. ein Fax oder eine E-Mail, unter Einsatz eines Algorithmus einem eindeutigen Prüfsummenverfahren unterzogen wird, um in Zukunft das Dokument identifizieren zu können.

[0046] Ein weiteres Verfahren der Erfindung sorgt für die rasche Identifizierung eines Individuums anhand der Untersuchung seiner biometrischen Probe und seines persönlichen Identifizierungscodes, indem mehrere unähnliche biometrische Proben aus unterschiedlichen Individuen in einem elektronischen Korb gespeichert werden, der durch einen persönlichen Identifizierungscode identifiziert ist.

[0047] In einer Ausführungsform der Erfindung ermöglicht es das Computersystem Individuen, ihren eigenen persönlichen Identifizierungscode (oder „PIC") aus einer Gruppe von PICs auszuwählen, die vom entfernt gelegenen Datenverarbeitungszentrum ausgewählt sind. Dies erfolgt durch ein Verfahren, in dem – sobald die biometrische Probe des Individuums erfasst ist – das Datenverarbeitungszentrum mehrere PICs wahllos auswählt, die man sich leicht merken kann. Das Datenverarbeitungszentrum führt dann einen Vergleich der erfassten biometrischen Probe mit jenen durch, die sich bereits in den PIC-Körben oder -Gruppen befinden. Sollte die biometrische Probe eines neuen Anmelders einer bereits registrierten biometrischen Probe ähneln, die einer der wahllos ausgewählten PIC-Gruppen zugeteilt wurde, wird dieser PIC von der Datenbank ausgeschieden und kann vom neuen Individuum nicht verwendet werden; es wird für einen weiteren derartigen biometrischen Vergleich ein alternativer PIC ausgewählt. Sobald das Datenverarbeitungszentrum mehrere PIC-Optionen ohne eine verwechslungsfähige ähnliche biometrische Probe erstellt hat, werden diese PICs dem neuen Anmelder präsentiert, und das Individuum kann dann aus ihnen einen PIC auswählen.

[0048] In einer Ausführungsform der Erfindung liegt ein Verfahren zur schnellen Suche zumindest einer zuvor

gespeicherten biometrischen Probe aus einem ersten Individuum vor, wobei hier ein PIC-Korb verwendet wird, der zumindest eine algorithmisch eindeutige zweite biometrische Probe enthält, die aus zumindest einem zweiten Individuum stammt und die vom PIC-Korb identifiziert wird, erstens umfassend einen Speicherschritt, der das Folgende umfasst: a) gegebenenfalls die Auswahl eines privaten Codes durch ein erstes Individuum; b) die Auswahl eines PIC durch das erste Individuum; c) das Eingeben einer biometrischen Probe aus dem ersten Individuum; d) das Lokalisieren des PIC-Korbs, der durch den durch das erste Individuum ausgewählten PIC identifiziert ist; e) Vergleichen der biometrischen Probe aus dem ersten Individuum mit allen zuvor gespeicherten biometrischen Proben im PIC-Korb, um sicherzustellen, dass sich die vom ersten Individuum eingegebene Probe algorithmisch eindeutig von der zuvor gespeicherten zumindest einen biometrischen Probe unterscheidet, die von zumindest einem zweiten Individuum stammt; und f) das Speichern der eingegebenen biometrischen Probe aus dem ersten Individuum im ausgewählten PIC-Korb, wenn sich die Probe algorithmisch von der zumindest einen gespeicherten biometrischen Probe aus dem zumindest einen zweiten Individuum unterscheidet. Es wird auch ein Bid-Schritt durchgeführt, umfassend: a) das Eingeben des ausgewählten PIC durch das erste Individuum; und b) das Eingeben einer biometrischen Probe durch das erste Individuum. Es wird auch ein Vergleichsschritt durchgeführt, umfassend: a) das Finden des PIC-Korbs, der durch den vom ersten Individuum eingegebenen PIC identifiziert ist; und b) das Vergleichen der eingegebenen biometrischen Probe aus dem ersten Individuum mit der zumindest einen gespeicherten biometrischen Probe aus dem zumindest einen zweiten Individuum im eingegebenen PIC-Korb, um entweder ein erfolgreiches oder ein fehlgeschlagenes Identifizierungsergebnis zu erzielen. Es könnte ferner Folgendes durchgeführt werden: a) ein Ausführungsschritt, in dem ein Befehl verarbeitet und ausgeführt wird, um eine Bestimmung zu liefern; b) ein Ausgabeschritt, in dem das Identifizierungsergebnis oder die Bestimmung externalisiert und angezeigt wird; und c) ein Präsentationsschritt, in dem nach erfolgreicher Identifizierung des ersten Individuums der private Code dem ersten Individuum präsentiert wird.

[0049] Gemäß einer Ausführungsform der Erfindung ist das Hostsystem in Reihe zwischen dem gerade identifizierten Individuum und anderen Computernetzwerken positioniert, auf die zugegriffen werden soll, und dient somit als Schnittstelle. Man beachte, dass in dieser Ausführungsform der Benutzer eine Zugriffsaufforderung direkt an das Hostcomputersystem der Erfindung stellt, die operativ mit anderen unabhängigen gesicherten Computersystemen wie z. B. VISANET interaktiv ist. Das Computersystem würde daher authentifizierte biometrischen Datenproben für alle autorisierten Benutzer jedes gesicherten und von ihm betriebenen Computersystems warten. Diese Daten würden von jedem autorisierten Benutzer gegengeprüft. Somit liefert nach dem Abschluss der Identitätsverifizierung das Sicherheitssystem dem Benutzer eine Auflistung von Systemen, zu deren Zugriff er autorisiert ist, und fordert den Benutzer auf, das erwünschte Netzwerk auszuwählen. Anschließend werden der angeforderte Ausführungsschritt und Informationen betreffend die Transaktion an das ausgewählte unabhängige Computernetzwerk weitergeleitet; dies ähnelt vom Typ her jenen Kommunikationen, die heute zwischen Kreditkartenvertragspartnern und -firmen versendet werden.

[0050] In einer zweiten Ausführungsform kann das Hostsystem die Funktionen der anderen unabhängigen Computersysteme wie z. B. das Verbuchen von Last- oder Gutschriften auf einem Finanzkonto durchführen. In diesem System führt das Computersystem der Erfindung die Funktionen aus, die das Individuum anfordert; dies erfolgt ohne Verwendung externer, unabhängiger Computernetzwerke.

[0051] Gemäß einer weiteren Ausführungsform der Erfindung ist ein Mittel zur Benachrichtigung von im Vorhinein angegebenen Behörden vorgesehen, während ein Zugriffsversuch erfolgt, bei dem der Benutzer von einem Dritten genötigt wurde, den Zugriff auf das Hostcomputersystem anzufordern. In einer derartigen Ausführungsform würde ein autorisierter Benutzer eine Reihe an Codes besitzen, von denen die meisten vom Computersystem als Standardzugriffscodes und andere als Notfallscodes erkannt würden. Das Vergleichsmittel des Computersystems wäre konfiguriert, zumindest einen Code pro autorisierten Benutzer anzunehmen und zu erkennen, und das Notfallsalarmmittel zu aktivieren, wenn der vom Benutzer eingegebene Code einem Notfallscode entspricht. Gleichzeitig würde die Bestimmung einer autorisierten Identität für den Benutzer dazu führen, dass der Benutzer Zugriff auf das angeforderte gesicherte Computersystem erhält – möglicherweise erfolgt dies auf einer Zugriffsebene, die in vorbestimmter Weise eingeschränkt ist, oder führt zur Anzeige irreführender Daten (z. B. „falscher Bildschirmanzeigen"), wodurch der nötigende Dritte nicht erkennen kann, dass eine Notfallsbenachrichtigung durch den Benutzer eingegeben wurde. Der Notfallscode würde dann als Teil des oder gleichzeitig mit dem PIC des Benutzers oder durch Auswahl eines Notfallskontoindex während des Zugriffs auf das Computersystem eingegeben. In beiden Fällen könnte das Wohlergehen des den Zugriff anfordernden Benutzers gefährdet sein, wenn der nötigende Dritte erkennen sollte, dass der Benutzer versucht, die Behörden zu verständigen. Somit ist es entscheidend, dass das Zugriffsverfahren ohne Unterbrechungen abläuft und dass einem autorisierten Benutzer Zugriff gewährt wird, so dass der nötigende Dritte davon ausgeht, dass alles normal vonstatten geht. Obwohl diese Merkmale in das Hostcomputernetzwerk der Erfindung

eingebaut sein können, ist es auch möglich, dass ein unabhängiges Computernetzwerk die gleichen oder modifizierte Versionen der oben erwähnten Merkmale ablaufen lässt.

[0052] Die Erfindung ist in unterschiedlicher Hinsicht dem Stand der Technik überlegen. Erstens ist das System für den Benutzer äußerst einfach und wirkungsvoll, insbesondere wenn der Benutzer auf Finanzkonten zugreift, da es nicht mehr erforderlich ist, Tokens mit sich zu tragen und zu präsentieren, um auf seine Konten zugreifen zu können. Dank der Erfindung ist es nicht mehr erforderlich, erwünschte Tokens mit sich zu tragen, sicher zu verwahren und zu lokalisieren, was viele Nachteile mit sich brachte. Da ferner Tokens oft für ein bestimmtes Computersystem spezifisch sind, das es außerdem erforderlich macht, dass man sich einen einem bestimmten Token zugewiesenen Geheimcode merkt, macht die vorliegende Erfindung alle solche Tokens überflüssig, wodurch die notwendige Merkleistung und der Aufwand für Konsumenten deutlich verringert wird, indem Zugriff auf alle Konten mit nur einem PIC ermöglicht wird. Somit kann der Konsument in einer einzigen Transaktion ohne Token praktisch jede kommerzielle Tätigkeit durchführen oder praktisch jede elektronische Nachricht versenden – er kann z. B. Geld von einem Bankkonto abheben, sein Einverständnis zu Vertragsbedingungen geben, Einkäufe über das Fernsehen tätigen, Vermögenssteuer zahlen usw. Der Konsument wird nun dank der Erfindung erstmals in die Lage versetzt, seine privaten und/oder beruflichen elektronischen Übertragungen und Transaktionen zu jedem beliebigen Zeitpunkt durchzuführen und ist dabei nicht mehr von Tokens abhängig, die gestohlen, beschädigt oder verloren gehen können.

[0053] Die Erfindung ist auch hinsichtlich des praktischen Nutzens für Einzelhändler und Finanzinstitutionen vorteilhaft, da Käufe und andere Finanztransaktionen weniger aufwendig und spontaner vorgenommen werden können. Die durch Finanztransaktionen anfallende Papiermenge ist im Vergleich zu aktuellen Systemen, bei denen getrennte Belege für das Kreditkartenunternehmen, den Vertragspartner und den Konsumenten erstellt werden, deutlich geringer. Solche elektronischen Transaktionen ersparen Händlern und Banken viel Zeit und Kosten, indem die operativen Ausgaben deutlich gesenkt werden. Da das System der Erfindung ausgelegt ist, dem Konsumenten direkten Zugriff auf alle seine Finanzkonten zu gewähren, ist es viel weniger oft notwendig, Transaktionen mit Geld, Schecks, Handelsdokumenten u. dgl. durchzuführen, wodurch die Kosten für Geräte und Mitarbeiter eingespart werden können, die solche Transaktionen erfassen und belegen müssen. Außerdem entfallen hohe Herstellungs- und Vertriebskosten für die Ausgabe und Neuausgabe von Kreditkarten, Kontokarten, Telefonkarten u. dgl., wodurch Händler, Banken und letztlich auch die Konsumenten viel Geld sparen. Das System der Erfindung kann wahrscheinlich auch das Wirtschaftswachstum unterstützen, da alle elektronischen Ressourcen eines Konsumenten lediglich durch Eingabe seines Fingerabdrucks oder anderer biometrischer Daten zur Verfügung stehen.

[0054] Die Erfindung ist gegenüber bestehenden Systemen auch insofern klar überlegen, als sie äußerst betrugssicher ist. Wie oben besprochen, sind aktuelle Computersysteme von Vornherein unzuverlässig, da bei ihnen die Bestimmung der Benutzeridentität auf dem physischen Vorweis eines eindeutigen produzierten Objekts sowie – in manchen Fällen – auf der Eingabe von dem Benutzer bekannten Informationen beruht. Leider kann aber sowohl der Token als auch die Information auf eine andere Person übertragen werden (durch Verlust, Diebstahl oder durch freiwilliges Handeln des autorisierten Benutzers). Sofern sich der autorisierte Benutzer nicht des Verlusts oder der unbeabsichtigten Übertragung des Tokens bzw. der Informationen bewusst ist und diese Vorfälle meldet, wird jeder, der in den Besitz des Tokens bzw. der Informationen gelangt, von bestehenden Sicherheitssystemen als autorisierter Benutzer erkannt, dem dieser Token und diese Informationen zugewiesen wurden.

[0055] Die Erfindung schaltet im Gegensatz dazu die Gefahr praktisch aus, dass nicht autorisierte Benutzer Zugriff erhalten, indem die Benutzeridentität anhand einer Analyse einer oder mehrerer eindeutiger biometrischer Eigenschaften ermittelt wird. Selbst im sehr seltenen Fall der Nötigung, in dem ein autorisiertes Individuum von einer nötigenden Person gezwungen wird, auf seine Konten zuzugreifen, antizipiert das System einen Notfallskontoindex, wodurch der autorisierte Benutzer die Behörden von dieser Übertretung unterrichten kann, ohne dass die nötigende Person davon erfährt.

[0056] Die Erfindung erhöht außerdem die Betrugssicherheit, indem Authentifizierungsdaten gewartet und die Vorgänge zur Identitätsverifizierung an einem Punkt im System durchgeführt werden, der operationell vom den Zugriff anfordernden Benutzer isoliert ist, wodurch der Benutzer daran gehindert wird, Kopien der Authentifizierungsdaten zu erhalten oder den Verifizierungsprozess zu beeinträchtigen. Ein solches System ist bestehenden Token-basierten Systemen klar überlegen, in denen Authentifizierungsinformationen, z. B. persönliche Codes, auf dem Token gespeichert sind und von diesem entfernt werden können und die tatsächliche Identitätsbestimmung während des Zugriffs potenziell in operativem Kontakt mit dem Benutzer steht.

[0057] Es ist daher ein Ziel der Erfindung, ein Computerzugriffs-Identifizierungssystem bereitzustellen, mit dem ein Benutzer nicht mehr ein physisches Objekt wie z. B. einen Token besitzen und vorweisen muss, um eine Systemzugriffsaufforderung einzuleiten.

[0058] Ein weiteres Ziel der Erfindung ist die Bereitstellung eines Computerzugriffs-Identifizierungssystems, das zur Verifizierung einer Benutzeridentität fähig ist, anstelle der Verifizierung des Besitzes proprietärer Objekte und Informationen.

[0059] Ein zusätzliches Ziel der Erfindung ist die Verifizierung der Benutzeridentität auf der Basis einer oder mehrerer eindeutiger Eigenschaften, die physisch auf den Benutzer zutreffen.

[0060] Ein weiteres Ziel der Erfindung ist die Bereitstellung eines Systems zum gesicherten Zugriff auf ein Computersystem, das praktisch, bequem und benutzerfreundlich ist.

[0061] Ein zusätzliches Ziel der Erfindung ist die Bereitstellung eines Systems zum gesicherten Zugriff auf ein Computersystem, das gegenüber betrügerischen Zugriffsversuchen seitens nicht autorisierter Benutzer sehr sicher ist.

[0062] Ein weiteres Ziel der Erfindung ist die Bereitstellung eines Computerzugriffs-Identifizierungssystems, das es dem Benutzer ermöglicht, Behörden davon in Kenntnis zu setzen, dass eine bestimmte Zugriffsaufforderung von einem Dritten mit Zwang durchgesetzt wird, ohne dass dieser Dritte von dieser Meldung erfährt.

[0063] Es besteht auch die Notwendigkeit, ein Computerzugriffs-Identifizierungssystem zu entwickeln, das je nach der vom Benutzer erwünschten Konfiguration die Transaktionsfähigkeiten des Benutzers im Rahmen des Computersystems automatisch einschränkt.

[0064] Diese und andere Vorteile der Erfindung ergeben sich aus der folgenden ausführlichen Beschreibung der Erfindung in Verbindung mit den beiliegenden Abbildungen.

Kurze Beschreibung der Abbildungen

[0065] **Fig.** 1 ist ein Diagramm des Systems der vorliegenden Erfindung.

[0066] **Fig.** 2 ist ein Diagramm des Datenverarbeitungszentrums (Data Processing Center, DPC) sowie seiner internen Datenbanken und Ausführungsmodule.

[0067] **Fig.** 3 ist ein Diagramm des Kassen-Endgeräts, der biometrischen Eingabevorrichtung und ihrer Komponenten sowie der Zwischenschaltungen dazwischen.

[0068] **Fig.** 4 ist ein Flussdiagramm des Betriebs der biometrischen Eingabevorrichtung und des Endgeräts zur Erzeugung eines Anfragepakets.

[0069] **Fig.** 5 ist ein darstellendes Diagramm des Anfragepakets sowie der obligatorischen und optionalen Daten, die es enthält.

[0070] **Fig.** 6 ist ein darstellendes Diagramm des Antwortpakets sowie der obligatorischen und optionalen Daten, die es enthält.

[0071] **Fig.** 7 ist ein Flussdiagramm, das das Datenverschlüsselungs- und Datenversiegelungsverfahren in der biometrischen Eingabevorrichtung veranschaulicht.

[0072] **Fig.** 8 ist ein Flussdiagramm, das das Datenentschlüsselungs- und Gegenteilnehmer-Identifizierungsverfahren im DPC veranschaulicht.

[0073] **Fig.** 9 ist ein Flussdiagramm, aus dem das Datenverschlüsselungs- und Datenversiegelungsverfahren im DPC ersichtlich ist.

[0074] **Fig.** 10 ist ein Flussdiagramm, das die Registrierung eines Individuums während des Registrierungsverfahrens zeigt.

[0075] **Fig.** 11 ist ein Flussdiagramm, das das Verfahren der Identifizierung des Individuums und der Rückübertragung des privaten Codes an das Individuum veranschaulicht.

[0076] **Fig.** 12 ist ein Flussdiagramm des Verfahrensablaufs im DPC und im Ausführungsschritt.

[0077] **Fig.** 13 ist ein Flussdiagramm des Notfallsanfrage- und Antwortverfahrens im DPC.

[0078] **Fig.** 14 ist ein Flussdiagramm des allgemeinen Betriebs der Handelstransaktionsautorisierungs-Ausführung im DPC.

[0079] **Fig.** 15 ist ein Flussdiagramm des allgemeinen Betriebs des Ferntransaktionsautorisierungs-Ausführungsschritts im DPC.

[0080] **Fig.** 16 ist ein Flussdiagramm des allgemeinen Betriebs der Geldausgabeautomat-Kontozugriffsausführung im DPC.

[0081] **Fig.** 17 ist ein Flussdiagramm des allgemeinen Betriebs der Aussteller-Stapelmodifizierungsausführung im DPC.

[0082] **Fig.** 18 ist ein Flussdiagramm des allgemeinen Betriebs der Ausführung der sicheren Vorlage von Faxnachrichten und elektronischen Dokumenten im DPC.

[0083] **Fig.** 19 ist ein Flussdiagramm des allgemeinen Betriebs der Ausführung sicherer Faxdaten und elektronischer Dokumentdaten im DPC.

[0084] **Fig.** 20A ist ein darstellendes Diagramm des Anfragepakets für elektronische Signaturen.

[0085] **Fig.** 20B ist ein darstellendes Diagramm des Antwortpakets für elektronische Signaturen.

[0086] **Fig.** 20C ist ein darstellendes Diagramm des Anfragepakets zur Verifizierung elektronischer Signaturen.

[0087] **Fig.** 20D ist ein darstellendes Diagramm des Anfragepakets zur Verifizierung elektronischer Signaturen.

[0088] **Fig.** 21 ist ein Flussdiagramm des allgemeinen Betriebs der Ausführung elektronischer Signaturen im DPC.

[0089] **Fig.** 22 ist ein Flussdiagramm des allgemeinen Betriebs der Verifizierungsausführung elektronischer Signaturen im DPC.

Ausführliche Beschreibung der Abbildungen

[0090] Wie bereits erwähnt, besteht das Hauptziel der Erfindung darin, ein Token-loses, sicheres, zuverlässiges und konsistentes Gerät und Verfahren zur Identifizierung von Individuen zwecks Durchführung von Finanztransaktionen und von Nicht-Finanz-Übertragungen bereitzustellen, das von einer großen Anzahl an Benutzern verwendet werden kann. Es ist das Wesen der Erfindung, dass Konsumenten die Möglichkeit besitzen, diese Transaktionen ohne Tokens, Kreditkarte, Ausweiskarten oder Identifizierungskarten wie z. B. Führerscheine durchführen können. Um funktionell zu sein, ist es entscheidend, dass das System bei Geschwindigkeiten betrieben wird, die zur Abwicklung von Finanztransaktionen wie z. B. von Kreditkartenkäufen und Geldausgabeautomatdiensten (ATM), die mehrere Banken und Kreditkonten betreffen, notwendig sind. Das System muss sicher sein, sodass die Aufzeichnungen bzw. Einträge des Individuums sowie seine biometrischen Informationen vertraulich behandelt und geschützt werden – sowohl innerhalb des Computersystems, das das Individuum identifiziert und Transaktionen autorisiert, als auch während der Datenübertragung zwischen dem Computersystem und entfernten Standorten, mit denen das Computersystem kommuniziert. Außerdem muss das System insofern zuverlässig sein, als Identifizierungs- und Autorisierungsfehler das System nicht beeinträchtigen oder verkomplizieren dürfen. Da nur die Verwendung biometrischer Daten zur Identifizierung von Individuen in Betracht gezogen wird, muss das System auch Sicherheitsmerkmale aufweisen, um entweder den Zugriff sogar seitens autorisierter Benutzer einzuschränken oder im Notfall die Behörden zu verständigen. Es ist zu beachten, dass das System eine große Anzahl an Benutzern bedienen und beträchtliche Datenmengen

speichern und übertragen muss, z. B. biocharakteristische Informationen, und dies bei Geschwindigkeiten, mit denen heute üblicherweise Finanztransaktionen abgewickelt werden.

[0091] Bezug nehmend auf die Abbildungen ist die allgemeine Konfiguration der Erfindung und ihrer Komponenten in **Fig.** 1 dargestellt. Ein Datenverarbeitungszentrum (DPC, Data Processing Center) **1** ist durch verschiedene Arten von Kommunikations- bzw. Übertragungsmitteln **3** mit verschiedenen Endgeräten **2** verbunden. Das DPC ist auch mit unabhängigen Computernetzwerken **4** verbunden und kommuniziert mit ihnen. Das DPC enthält zahlreiche Datenbanken und Softwareausführungsmodule, die aus **Fig.** 2 ersichtlich sind. In einer bevorzugten Ausführungsform der Erfindung werden die Datenbanken aus Sicherheitsgründen gesichert oder „gespiegelt". Die Firewall-Einheit **5** ist dafür verantwortlich, das elektronische Eindringen in das System zu verhindern, während die Gateway-Einheit **6** für die Durchführung aller Anforderungen des Benutzers zuständig ist, z. B. für das Hinzufügen, Löschen oder Modifizieren sämtlicher Datenbanken. Die Gateway-Einheit ist auch für das Entschlüsseln und Entpacken von Daten aus den Endgeräten verantwortlich; dies erfolgt mittels des MACM-Moduls **7**, des MDM-Moduls **8** und den SNM-Moduls **9**. Das PGL-Modul **10** und das IML-Modul **11** dienen dazu, den richtigen persönlichen Identifizierungscode und den Korb der biometrischen Probe zu lokalisieren. **Fig.** 3 zeigt ein Beispiel für ein Endgerät und die biometrische Eingabevorrichtung **12**, die einen biometrischen Scanner bzw. eine biometrische Abtastvorrichtung **13**, ein Dateneingabemittel wie z. B. ein Tastenfeld oder PIN-Feld **14** und ein Anzeigefeld **15** aufweist. Der biometrische Scanner kann ein Fingerdruck-, Stimmerkennungs-, Handflächenabdruck-, Netzhautscanner o. dgl. sein, obwohl als Beispiel hier ein Fingerdruckscanner eingesetzt wird. Die biometrische Eingabevorrichtung ist außerdem mit Berechnungsmodulen **16**, Gerätetreibern und löschbaren sowie nicht löschbaren Speichermodulen ausgestattet. Die biometrische Eingabevorrichtung ist weiters mit Computer-Modulen **16**, Gerätetreibern und löschbaren sowie nicht-löschbaren Speichermodulen ausgestattet. Die biometrische Eingabevorrichtung kommuniziert mit dem Endgerät vorzugsweise durch eine serielle Schnittstelle **17**. Das Endgerät **2** kommuniziert mit dem DPC **1** durch ein herkömmliches Modem **18** mithilfe von Anfragepaketen **19** und Antwortpaketen **20** sowie eines der Zwischenschaltungsmittel in **Fig.** 1; Beispiele dafür sind Kabelnetze, Mobiltelefonnetze, Telefonnetze, das Internet, ein ATM-Netzwerk oder X.25. **Fig.** 4 ist ein darstellendes Diagramm des Anfragepakets **19** und seines Verfahrens zur Erzeugung der Software für die biometrische Eingabevorrichtung. **Fig.** 5 und 6 sind darstellende Diagramme des Anfragepakets und des Antwortpakets mit optionalen und obligatorischen Datensegmenten. Außerdem sieht man, welche Teile der Pakete verschlüsselt und welche versiegelt sind. **Fig.** 7 ist ein Blockdiagramm des allgemeinen Verfahrens zur Datenverschlüsselung und -versiegelung, wobei man die Verwendung von DUKPT-Schlüsseldaten **20** für die Verschlüsselung von Daten vor dem Hinzufügen zusätzlicher Daten vor der Versiegelung des Anfragepakets mit einem Nachrichten-Authentifizierungscodeschlüssel (MCA, Message Authentication Code Key) **21** erkennt. **Fig.** 8 und 9 zeigen das Entschlüsselungs- und Verschlüsselungsverfahren im DPC. **Fig.** 12–19 sowie **Fig.** 21–22 sind Blockdiagramme ausgewählter Beispiele für im DPC erfolgende Ausführungsschritte.

[0092] Es folgen eine Beschreibung der Abbildungen, Diagramme, Flussdiagramme sowie eine ausführliche Erläuterung der Erfindung einschließlich ihrer Hardwarekomponenten, Softwarekomponenten, Ausführungsmodule, Datenbanken, Verbindungsmittel, der Datenübertragung dazwischen und des erfindungsgemäßen Verfahrens.

1.1. Biometrische Eingabevorrichtung (BIA, Biometric Input Apparatus)

1.1.1. Einführung

[0093] Die BIA ist eine Kombination von Hardware und Software, deren Aufgabe darin besteht, biometrische Eingaben für die Identifizierung von Individuen zu erfassen, zu codieren und zu verschlüsseln. Alle Tätigkeiten der BIA werden von einer externen Kontrolleinheit, einem so genannten Endgerät, gesteuert, das Befehle ausgibt und die Ergebnisse über die serielle Verbindung der BIA erhält.

[0094] Die BIA-Hardware liegt in vier Grundversionen vor: Standard, drahtlos, integriertes Telefon/Kabelfernsehen (bzw. „CATV")/Fax und ATM. Jede BIA-Hardwarevariante ist speziell für eine bestimme praktische Anwendung entwickelt worden, und aufgrund konstruktiver Unterschiede verfügt jede Variante über ein unterschiedliches Sicherheitsniveau.

[0095] Von der BIA-Software existieren sieben Grundversionen: PC, Einzelhandel, Geldausgabeautomat (ATM), Registrierung, intern, Ausgabe und fernintegriert. Jedes Softwarepaket bietet einen Satz unterschiedlicher Benutzer-spezifischer Befehle. Beispielsweise akzeptiert das Registrierungssoftwarepaket keine Aufforderungen, Einzelhandelstransaktions-Nachrichten zu erstellen; die Befehle der Einzelhandelssoftware können

keine individuellen Registrierungsnachrichten übermitteln. Um eine weitere Sicherheitsstufe einzubauen, ist dafür gesorgt, dass das DPC weiß, welches Softwarepaket in jede BIA geladen wurde; jeder Versuch einer BIA, eine Nachricht zu verschicken, die normalerweise nicht übermittelt werden kann, wird abgewiesen und als schwerer Verstoß gegen die Sicherheitsvorschriften behandelt.

[0096] Die Fähigkeit des erfindungsgemäßen Systems, Betrug im Geschäftslokal des Vertragspartners zu erkennen und zu bekämpfen, beruht auf der Tatsache, dass die externe Schnittstelle der BIA streng limitiert ist, dass die Konstruktion der BIA unerlaubte Zugriffe auf den Inhalt extrem erschwert, dass jede BIA über ihre eigenen eindeutigen Verschlüsselungscodes verfügt, die nur dem DPC bekannt sind, und dass jede BIA nur jene Vorgänge durchführen kann, die ihren definierten Funktionen entsprechen. Jedes biometrische Eingabemittel besitzt einen Hardware-Identifizierungscode, der zuvor im DPC registriert wurde, wodurch das biometrische Eingabemittel für das DPC in jeder späteren von dieser BIA ausgehenden Übertragung eindeutig identifizierbar ist.

[0097] Bei der Entwicklung der BIA ging man davon aus, dass das Steuerendgerät betrugsanfällig ist. Endgeräte reichen von Softwareapplikationen auf PCs bis zu dedizierten Hardware/Softwaresystemen, die für einen bestimmten Verwendungszweck entwickelt wurden, z. B. in Geschäftslokalen. Ungeachtet des jeweiligen Modells legt keine BIA unverschlüsselte biometrische Informationen offen. BIA-Modelle ohne Anzeigemittel (z. B. LCD, LED oder Quarzschirme) müssen ausgewählte Informationen (z. B. individuelle private Codes) dem Endgerät zur Anzeige übermitteln, weshalb diese Endgerät-BIA-Kombinationen als weniger sicher eingestuft werden.

[0098] Je nach der konkret durchzuführenden Aufgabe sind BIA-Modelle entweder partiell oder komplett mit dem Endgerät integriert. Partiell integrierte Geräte sind physikalisch vom Endgerät getrennt; und sie beinhalten drahtlose und standardmäßige BIAs für Geschäftslokale. Vollintegrierte Geräte sind innerhalb des Endgeräts selbst enthalten, z. B. in Geldausgabeautomaten (ATM) oder Telefonen.

[0099] Keine BIA legt jemals geheime Verschlüsselungscodes gegenüber einer externen Quelle offen.

1.1.2. BIA-Modelle

[0100] Bestimmte BIA-Hardwaremodelle besitzen unterschiedliche Konfigurationen. Sie sind nachstehend kurz beschrieben.

BIA

[0101] Standardmodell mit Berechnungsmodul (z. B. Multichipmodule), biometrischem Scanner (d. h. Einzelfingerabdruck-Scanner), Anzeigemittel (d. h. LCD-Schirm), Kommunikationsanschluss (d. h. serielle Schnittstelle), Dateneingabemittel (d. h. Tastatur zur manuellen Dateneingabe oder PIC-Feld) innerhalb eines unerlaubten Zugriff verhindernden Gehäuses und elektronischem Detektionsmittel (d. h. HF-Abschirmung).

BIA/Drahtlos

[0102] Standardmodell, doch die serielle Verbindung ist durch ein drahtloses Spreizspektrum-Kommunikationsmodul mit externer Antenne ersetzt. Kommt in Gastronomiebetrieben zum Einsatz.

BIA/Geldausgabeautomat (ATM)

[0103] Besitzt Hochleistungsscanner und serielle Schnittstelle sowie ein Multichipmodul. Die Tatsache, dass die LCD Teil des Endgeräts und nicht der BIA ist, bedeutet niedrigere Sicherheit, da der private Code dem Endgerät übermittelt werden muss. Kommt in Geldausgabeautomaten (ATM) zum Einsatz.

BIA/CATV

[0104] Besitzt weniger leistungsstarken Scanner, sonst wie Geldausgabeautomat-Version. Kommt in Telefonen, CATV-Fernbedienungen und Faxgeräten zum Einsatz. Niedrigste Sicherheitsstufe, da die LCD und das PIC-Feld Teil des Endgeräts und nicht der BIA sind und aufgrund des niedrigen Preisniveaus auf dem Markt.

1.1.3. BIA-Befehle

[0105] Jeder Satz an BIA-Softwarebefehlen umfasst unterschiedliche Vorgänge. Es folgt eine Kurzbeschreibung.

BIA/Geldausgabeautomat

Kontozugriff

BIA/CATV

Ferntransaktions-Autorisierung

BIA/Fax

Sichere Faxvorlage
Sichere Faxdaten
Sichere Faxverfolgung
Sicherer Faxabruf
Sichere Faxabweisung
Sichere Faxarchivierung
Sichere Annahme des Faxvertrags
Sichere Ablehnung des Faxvertrags
Aufrufen archivierter elektronischer Dokumente

BIA/intern

Individuelle Identifizierung

BIA/Ausgabe

Ausgabe-Batch

BIA/PC

Vorlage elektronischer Dokumente
Daten elektronischer Dokumente
Verfolgung elektronischer Dokumente
Abruf elektronischer Dokumente
Abweisung elektronischer Dokumente
Archivieren elektronischer Dokumente
Abruf archivierter elektronischer Dokumente
Vorlage elektronischer Signaturen
Überprüfung elektronischer Signaturen
Fern-Transaktionsautorisierung
Netzwerk-Akkreditiv
Gesicherte Verbindung

BIA/Registrierung

Individuelle Identifizierung
Biometrische Registrierung

BIA/Einzelhandel

Transaktionsautorisierung

1.1.4. BIA-Hardware: Standardmodell

[0106] Die Standard-BIA-Hardware ist ein Multichipmodul kombiniert mit einem Einzeldruckscanner, einem

LCD-Schirm, einer seriellen Schnittstelle und einem PIC-Feld, das in einem original-gesichertern Hartgehäuse untergebracht ist, das den versuchten unerlaubten Zugriff meldet, während für den Inhalt HF-Abschirmung bereitgestellt ist.

[0107] Die folgenden Komponenten werden zu einem Multichipmodul zusammengefasst, das als BIA-Multichipmodul bezeichnet wird (dieses Verfahren zur Unterbringung mehrerer Prozessoren in einer physikalischen Hülle ist auf dem Gebiet allgemein bekannt) und ausgelegt ist, die Kommunikationswege zwischen den Geräten vor unerlaubtem Abhören zu schützen.

- Serieller Prozessor
- PIC-Feld-Prozessor
- LCD-Schirm-Prozessor
- CCD-Scanner-A/D-Prozessor
- Hochgeschwindigkeits-DSP-Prozessor mit Flash- und Masken-ROM
- Allzweck-Mikroprozessor
- Standard-RAM
- EEPROM

[0108] Die folgenden Softwarepakete und Daten sind in Masken-ROM gespeichert. Masken-ROM sind billiger als andere Arten von ROM, doch sie werden leicht umgekehrt (reverse engineered) und sind elektronisch nicht löschbar. Hier ist nur der nichtkritische allgemein verfügbare Code angeführt (Masken-ROM sind auf dem Gebiet der Erfindung allgemein bekannt).

- MAC-Berechnungsbibliothek
- DUKPT-Schlüsselverwaltungsbibliothek
- DES- oder (CBC-) Verschlüsselungsbibliothek
- Base-64 (8-bit-in-ausdruckbaren-ASCII) Konverterbibliothek
- Public Key-Verschlüsselungsbibliothek
- Eingebettetes Betriebssystem
- Treiber für serielle Leitung
- Treiber für LCD-Vorrichtung
- Treiber für PIC-Feld
- Treiber für Scannervorrichtung
- Eindeutiger Hardware-Identifizierungscode
- Vielfachsprachenprofile

[0109] Die folgenden Standarddaten und Softwarepakete sind in Flash-ROM gespeichert. Flash-ROM sind teurer, doch es ist das Umkehren (Reverse Engineering) bei ihnen schwieriger, und vor allem sind sie elektronisch löschbar. Alle kritischen Informationen sind hier gespeichert. Flash-ROM werden verwendet, um das Duplizieren einer BIA zu erschweren (Flash-ROM sind in der Industrie allgemein bekannt).

- Eindeutige DUKPT0-Tabelle zukünftiger Schlüssel
- Eindeutiger 112-bit MAC-Schlüssel
- DSP-Algorithmus zur Bestimmung der biometrischen Qualität
- DSP-Biometrik-Codieralgorithmus
- Algorithmus zum Generieren von Zufallszahlen
- Befehlsfunktionstabelle

[0110] Die Nachrichtsequenzzahl, die bei jedem Versand einer Nachricht aus der BIA inkrementiert wird, wird im EEPROM gespeichert. EEPROM kann mehrmals gelöscht werden, ist aber nichtflüchtig – der Inhalt bleibt auch nach Stromunterbrechungen gültig (EEPROM ist auf dem Gebiet der Erfindung allgemein bekannt).

[0111] Die folgenden Daten sind in RAM gespeichert. RAM sind von ihrer Beschaffenheit her temporär, und die Daten gehen bei jeder Stromunterbrechung verloren.

- Codiertes biometrisches Register
- PIC-Register
- Kontoindexcode-Register
- Titelindexcode-Register
- Betragsregister
- Dokumentnamen-Register
- PIC-Block-Schlüssel
- Nachrichtenschlüssel
- Antwortschlüssel

– Schlüssel für gemeinsame Sitzungen
– Schlüssel für private Sitzungen
– 8 allgemeine Register
– Raum zum „Stapeln und Aufhäufen"

[0112] Jedes Multichipmodul enthält eine einmal zu beschreibende Position, die nach der Initialisierung des Flash-ROM irreversibel gesetzt wird. Wenn versucht wird, Software in den Flash-ROM herunterzuladen, wird dieser Speicherplatz überprüft.

[0113] Wenn er bereits gesetzt wurde, verweigert die BIA den Ladevorgang. Auf diese Weise können kritische Software und Datenschlüssel nur einmal, zum Zeitpunkt der Herstellung, in die Vorrichtung geladen werden.

[0114] Alle Register und Schlüssel werden beim Abbruch einer Transaktion explizit auf null gesetzt. Sobald eine Transaktion abgeschlossen ist, werden die Biometrik-, PIC- und Kontoindexcode-Register sowie alle Verschlüsselungsschlüssel, die für die nachfolgende Verwendung nicht benötigt werden, gelöscht. Sobald ein „Nachricht bilden"-Befehl ausgeführt worden ist, werden biometrische, PIC- und Konto-Indexcode-Register auch gelöscht, gemeinsam mit jeglichen Verschlüsselungsschlüsseln, die für den nachfolgenden Gebrauch nicht erforderlich sind.

[0115] Es ist wichtig, dass die Software keine Kopien von Registern oder Schlüsseln in Stapelvariablen aufbewahrt (auf dem Gebiet der Erfindung bekannt).

[0116] Die folgenden zugeordneten Hardwarekomponenten umfassen das Standard-BIA-Hardwaremodul.
– BIA-Multichipmodul
– CCD-Einzeldruckscanner
– Kapazitätsdetektorplatte (auf dem Gebiet der Erfindung bekannt)
– Beleuchtetes PIC-Tastenfeld
– 2-Zeilen-40-Spalten-LCD-Schirm
– HF-Abschirmung
– Originalgesichertes Gehäuse
– Serielle Verbindung (bis zu 57,6 kb)
– Hardware zum Detektieren des Verstoßes von Sicherheitsvorschriften (auf dem Gebiet der Erfindung bekannt)
– Optionale am Multichipmodul angefügte Thermitladung (auf dem Gebiet der Erfindung bekannt)

[0117] Alle temporären Speicher- sowie internen Hardware- und Softwareprodukte, die zur Berechnung dieser Werte verwendet werden, sind gesichert, d. h. sie widerstehen Versuchen, ihre aktuellen Werte oder ihre Funktionsweise zu ermitteln. Dieses Merkmal ist in Bezug auf die Sicherheit der Erfindung wesentlich, und ebenso entscheidend ist es, dass das Abhören einer BIA, konkret das Erfassen eines Biometrik-PIC-Blocks mit betrügerischer Absicht, möglichst erschwert wird.

[0118] Das Multichipmodul und die Komponenten sind dort, wo es sinnvoll ist, physikalisch ohne offen zugängliche Verdrahtung miteinander verbunden.

[0119] Das Gehäuse zum Schutz der elektronischen Komponenten der BIA wird während der Herstellung zugeschweißt. Es kann unter gar keinen Umständen ohne beträchtliche Beschädigung geöffnet werden. Nach dem Detektieren des Öffnens (oder der Beschädigung) des Gehäuses führt die BIA eine elektronische Notfallsnullsetzung aller Schlüssel im Flash-ROM und anschließend aller Softwarebibliotheken durch. Die Verfahren zum Detektieren des unerlaubten Zugriffs werden als vertraulich und proprietär eingestuft.

[0120] Zusätzlich zum Schutz des Inhalts schirmt das Gehäuse die inneren Vorgänge auch von HF-Signaldetektoren ab.

[0121] Es bestehen auch hypersichere Versionen der BIA, in denen die Verfahren zum Detektieren eines unerlaubten Zugriffs mit einem Mechanismus verbunden sind, der das Multichipmodul sowie die Detektionsverfahren selbst physikalisch zerstört.

1.1.5. BIA-Hardware: Drahtloses Modell

[0122] Die drahtlose Version der BIA-Hardware ist mit dem in Konstruktion befindlichen Standardmodell iden-

tisch, außer dass ein drahtloses Spreizspektrum-Kommunikationsmodul unter Verwendung einer externen Antenne anstelle einer externen seriellen Schnittstelle exportiert wird.

[0123] Diese Version ist für den Gebrauch in Gastronomiebetrieben geeignet, wo Transaktionen dem Kundenwunsch entsprechend autorisiert werden.

[0124] In den folgenden Beschreibungen werden Elemente, die dem Standardsatz hinzugefügt sind, durch das „+"-Zeichen identifiziert; hingegen werden Elemente, die aus dem Standardsatz fehlen, durch das „–"-Zeichen identifiziert.

Multichipmodul

– Dokumentnamen-Register
– Schlüssel für gemeinsame Sitzungen
– Schlüssel für private Sitzungen
– Nachrichtenschlüssel

Komponenten

– Serielle Schnittstelle
+ Externe Antenne
+ Drahtloses serielles Spreizspektrummodul (auf dem Gebiet der Erfindung bekannt)

1.1.6. BIA-Hardware: Geldausgabeautomat (ATM)-Modell

[0125] Die Geldausgabeautomat-Version der BIA-Hardware ist ein mit einem Hochleistungs-Einzeldruckscanner und einer seriellen Schnittstelle kombiniertes Multichipmodul. Die Komponenten sind in einem zugriffssicheren Gehäuse untergebracht, das unerlaubten Zugriff meldet und für HF-Abschirmung des Inhalts sorgt.

[0126] Diese Version ist ausgebildet, auch nachträglich in Geldausgabeautomaten eingebaut zu werden. Das Scannerfeld ist ein Hochleistungssensorfeld, und die gesamte Konstruktion macht sich die bestehenden Schirme und Tastenfelder im Geldausgabeautomat (ATM) zunutze.

[0127] In den folgenden Beschreibungen sind Elemente, die zum Standardsatz hinzugefügt werden, mit dem „+"-Zeichen versehen, während Elemente, die im Standardsatz fehlen, mit dem „–"-Zeichen versehen sind.

Multichipmodul

– Betragsregister
– Dokumentnamen-Register
– Schlüssel für gemeinsame Sitzungen
– Schlüssel für private Sitzungen
– Nachrichtenschlüssel

Komponenten

– Beleuchtetes PIC-Tastenfeld
– 2-Zeilen-40-Spalten-LCD-Schirm

[0128] Es ist zu beachten, dass der Geldausgabeautomat keinen LCD-Schirm oder kein PIC-Tastenfeld besitzt und daher diese Gerätetreiber im Masken-ROM nicht erforderlich sind.

1.1.7. BIA-Hardware: Telefon/CATV-Modell

[0129] Die Telefon/CATV-Version der BIA-Hardware ist ein mit einem Einzeldruckscanner und einer seriellen Schnittstelle kombiniertes Multichipmodul. Das Modul ist physisch am Scanner befestigt, und die gesamte Struktur befindet sich in einem Kunststoffgehäuse, um unerlaubte Zugriffe zu erschweren. Für die Komponenten wird etwas HF-Abschirmung geboten.

[0130] Diese Version ist ausgebildet, mit Telefonen, Fernsehfernbedienungen und Faxgeräten integriert zu

werden. Sie bedient sich daher der bestehenden Tastenfelder und LCD-Schirme oder Fernsehschirme, um Werte einzugeben oder anzuzeigen. Ferner verwendet sie die Kommunikationseinrichtungen des Hostendgeräts. Beispielsweise benutzt das Faxgerät ein eingebautes Faxmodem und die Fernsehfernbedienung das CATV-Kabelnetz.

[0131] Dieses Hardwaremodell ist im Vergleich zu anderen Modellen relativ unsicher, da man darauf abzielt, dass diese Geräte so kostengünstig wie möglich sind, nicht viel wiegen und leicht in bestehende ebenfalls kostengünstige Geräte eingebaut werden können.

[0132] Natürlich sind Versionen mit höherem Sicherheitsniveau und besseren Gehäusen auch möglich und gemäß der Erfindung auch erwünscht.

[0133] In den folgenden Beschreibungen sind Elemente, die zum Standardsatz hinzugefügt werden, mit dem „+"-Zeichen versehen, während Elemente, die im Standardsatz fehlen, mit dem „–"-Zeichen versehen sind.

Multichipmodul

– Dokumentnamen-Register
– Schlüssel für gemeinsame Sitzungen
– Schlüssel für private Sitzungen
– Nachrichtenschlüssel

Komponenten

– Beleuchtetes PIC-Tastenfeld
– 2-Zeilen-40-Spalten-LCD-Schirm

1.2. BIA-Software

1.2.1. BIA-Software-Befehlsschnittstelle

[0134] Die externe Schnittstelle zur BIA ähnelt jener eines Standardmodems; Befehle werden von einem Steuerendgerät aus an sie übermittelt, wobei hier eine externe serielle Leitung zur Anwendung kommt. Wenn ein Befehl abgeschlossen ist, wird ein Antwortcode von der BIA an das Endgerät geschickt.

[0135] Jedes BIA-Softwarepaket unterstützt einen anderen Satz an Vorgängen. Beispielsweise unterstützt ein Geschäftslokalpaket nur Transaktionsautorisierungen, während ein Registrierungspaket die Identifizierung und biometrische Registrierung des Individuums unterstützt.

[0136] Alle BIA-Datenfelder sind ASCII-druckbar, wobei Felder durch ein Feldtrenner-(„fs", field separator) Steuerzeichen und Einträge durch neue Zeilen voneinander getrennt sind. Verschlüsselte Felder werden mittels der Basis-64-Konversionsbibliothek in 64-bit-ASCII binär umgewandelt (alle Produkte auf dem Gebiet der Erfindung bekannt).

[0137] Einige Befehle stehen in gewissen Konfigurationen nicht zur Verfügung. Beispielsweise kann die Geldausgabeautomat-BIA „PIC Erhalten" nicht unterstützen, da es kein angeschlossenes PIC-Feld gibt. Stattdessen unterstützt die Geldausgabeautomat-BIS einen „PIC Setzen"-Befehl.

Antwortcodes

Zeit abgelaufen

[0138] Die für den Befehl zugeteilte Zeit ist abgelaufen. Eine diesbezügliche Nachricht wird auf dem allenfalls vorhandenen LCD-Schirm angezeigt. Wenn die Zeit für einen bestimmten Befehl abgelaufen ist, agiert die BIA so, als ob der Stornoknopf betätigt wurde.

Storniert

[0139] Der „Storno"-Knopf wurde gedrückt, und der gesamte Vorgang wird abgebrochen. Die Nebenwirkung davon ist, dass alle erfassten Informationen gelöscht werden. Eine diesbezügliche Nachricht wird auf dem al-

lenfalls vorhandenen LCD-Schirm angezeigt.

OK

[0140] Der Befehl war erfolgreich.

Andere

[0141] Jeder Befehl kann spezifische andere Antwortcodes haben, die nur für ihn gültig sind. Diese Antwortcodes umfassen im Allgemeinen den Code begleitenden Text, der auf dem allenfalls vorhandenen LCD-Schirm angezeigt wird.

Nachricht

[0142] Dies zeigt an, dass der Befehl läuft, dass aber die BIA eine Nachricht mit dem Zwischenergebnis an das Endgerät schicken möchte. Das Ergebnis wird auch auf dem allenfalls vorhandenen LCD-Schirm angezeigt. Dieses Feature wird für Aufforderungen sowie für Statusnachrichtungen verwendet.

Befehle

[0143] In der nachstehenden Argumentliste umschließen die Zeichen <> individuelle Argumente, die Zeichen [] optionale Argumente und das Zeichen | gibt an, dass ein bestimmtes Argument aus einer der präsentierten Möglichkeiten bestehen kann.

Sprache einstellen <Sprache-Name>

[0144] Dieser Befehl wählt eine Sprache aus unterschiedlichen Sprachen aus, die innerhalb der BIA codiert sind, um dadurch den Benutzer zur Eingabe aufzufordern.

Biometrische Eingabe erhalten <Zeit> [primär|sekundär]

[0145] Dieser Befehl fordert die BIA auf, ihren Scanner zu aktivieren, um eine biometrische Eingabe vom Individuum zu erhalten und sie im codierten biometrischen Register zu speichern.

[0146] Zunächst wird die Nachricht „Bitte legen Sie einen Finger auf das beleuchtete Feld" auf dem LCD-Feld angezeigt und an das Endgerät zurückgeschickt. Das Scannerfeld wird beleuchtet, und das Individuum wird aufgefordert, seine biometrischen Daten einzugeben.

[0147] Ein <Zeit> Wert von null bedeutet, dass die Zeit für die Eingabe der biometrischen Daten nicht beschränkt ist.

[0148] Im Abtastmodus wird eine Fingerdruckabtastung vorgenommen und durch den Abdruckqualitäts-Algorithmus einer Voranalyse unterzogen. Wenn die Abtastung nicht zufrieden stellend ist, nimmt die BIA weiterhin Abtastungen vor, bis <Zeit> Sekunden vergehen. Im Lauf der Zeit werden Aufnahmen des Abdrucks gemacht und analysiert und Nachrichten auf dem LCD-Schirm angezeigt und an das Endgerät geschickt (in Abhängigkeit von den Problemen, die die Abdruckqualitäts-Software detektiert). Wenn kein Abdruck ausreichender Qualität erstellt wird, sendet die BIA einen Zeitablauffehlercode zurück, und es erscheint eine diesbezügliche Nachricht auf der LCD.

[0149] Sobald der Abdruckqualitäts-Algorithmus die Qualität der Abdruckabtastung bestätigt, werden die Abdruckdetails durch den Abdruckcodier-Algorithmus extrahiert. Nur ein Teilsatz der Details wird nach dem Zufallsprinzip ausgewählt, wobei darauf geachtet wird, dass zur Identifizierung genügend Details vorliegen. Diese Details werden dann zufällig geordnet und in das codierte biometrische Register gestellt. Dann antwortet die BIA mit dem Code für ein erfolgreiches Ergebnis.

[0150] Wenn [primär|sekundär] angegeben ist (nur im biometrischen Registrierungs-Befehlsatz verfügbar), wird der gesamte Detailsatz ausgewählt, nicht nur der kleinere Teilsatz. Die primäre/sekundäre biometrische Selektion setzt schließlich auch die biometrischen Daten in das geeignete Register.

[0151] Gleichgültig ob der Vorgang erfolgreich abgeschlossen wurde oder nicht, wird das Licht, das den lau-

fenden Abtastvorgang anzeigt, ausgeschaltet, sobald das Abtasten beendet ist.

[0152] Es ist sehr wichtig, dass dieselbe biometrische Eingabe unterschiedliche Codierungen nach sich zieht, um so die Aufgabe jeder Person zu erschweren, die versucht, die Verschlüsselungscodes einer entwendeten BIA zu knacken. Dies erfolgt durch Auswahl eines zufälligen Teilsatzes und durch Zufallsordnen der codierten biometrischen Eingabe.

PIC Erhalten <Zeit>

[0153] Dieser Befehl fordert die BIA auf, das PIC-Register durch Ablesen vom Tastenfeld zu füllen.

[0154] Zunächst wird die Nachricht „Bitte geben Sie Ihren PIC ein und drücken sie dann <enter>" auf dem LCD-Schirm angezeigt und an das Endgerät übermittelt; dann werden die entsprechenden Tastenfeldlichter eingeschaltet, und das Abtasten des Tastenfelds kann beginnen.

[0155] Das Abtasten bzw. Scannen stoppt entweder nach <Zeit> Sekunden oder wenn das Individuum die „Enter"-Taste drückt.

[0156] Es ist zu beachten, dass einzelne Ziffern des PIC nicht auf dem LCD-Feld angezeigt werden. Für jede vom Individuum eingegebene Ziffer erscheint als Rückmeldung das Zeichen „*". Wenn die „Korrektur"-Taste gedrückt wird, wird die zuletzt eingegebene Ziffer gelöscht, und das Individuum kann den Eingabefehler beheben.

[0157] Wenn die PIC-Eingabe abgeschlossen ist, wird die Tastenfeldbeleuchtung ausgeschaltet.

[0158] Bei Erfolg sendet der Befehl OK.

Kontoindexcode Erhalten <Zeit>

[0159] Zunächst wird die Nachricht „Geben Sie nun Ihren Kontoindexcode ein und drücken Sie dann „Enter"" auf der LCD angezeigt und an das Endgerät gesendet. Dies fordert das Individuum auf, seinen Kontoindexcode einzugeben. Wenn jede Taste gedrückt wurde, erscheint dieser Wert auf dem LCD-Feld. Die Korrekturtaste kann gedrückt werden, um einen der Werte zu löschen. Wenn die Enter-Taste gedrückt wurde, wird das Kontoindexcode-Register gesetzt.

[0160] Während der Eingabe werden die entsprechenden Tasten auf dem Tastenfeld beleuchtet; nach Abschluss der Eingabe werden die Lichter auf dem Tastenfeld ausgeschaltet.

[0161] Bei Erfolg sendet der Befehl OK.

Titelindexcode Erhalten <Zeit>

[0162] Zunächst wird die Nachricht „Geben Sie nun Ihren Titelindexcode ein und drücken Sie dann „Enter"" auf der LCD angezeigt und an das Endgerät gesendet. Dies fordert das Individuum auf, seinen Titelindexcode einzugeben. Wenn jede Taste gedrückt wurde, erscheint dieser Wert auf dem LCD-Feld. Die Korrekturtaste kann gedrückt werden, um einen der Werte zu löschen. Wenn die Enter-Taste gedrückt wurde, wird das Titelindexcode-Register gesetzt.

[0163] Während der Eingabe werden die entsprechenden Tasten auf dem Tastenfeld beleuchtet; nach Abschluss der Eingabe werden die Lichter auf dem Tastenfeld ausgeschaltet.

[0164] Bei Erfolg sendet der Befehl OK.

Betrag Validieren <Betrag> <Zeit>

[0165] Der Befehl „Betrag validieren" (bestätigen) sendet die Nachricht „Betrag <Betrag> OK?" an das Endgrät und zeigt ihn auf dem LCD-Schirm an. Wenn das Individuum durch Drücken der Ja- oder Enter-Taste den Betrag bestätigt, wird das Betragsregister auf <Menge> gesetzt. Der <Betrag> Wert muss eine gültige Zahl ohne Steuerzeichen oder Leerzeichen usw. sein. Während der Aufforderung sind die Ja-, Nein- und Stornotasten beleuchtet. Sobald die Aufforderung abgeschlossen ist, werden alle Lichter ausgeschaltet.

[0166] Wenn das Individuum „nein" eingibt, wird der Vorgang abgebrochen.

Betrag Eingeben <Zeit>

[0167] Der Befehl „Betrag eingeben" sendet die Nachricht „Betrag eingeben" an das Endgerät und zeigt diese auf dem LCD-Schirm an. Das Individuum muss dann den Betrag in der jeweiligen Währung selbst eingeben. Jedes eingegebene Zeichen wird auf dem LCD-Schirm angezeigt. Alle notwendigen Tasten leuchten. Wenn die Enter-Taste gedrückt wird, wird das Betragsregister auf den auf der Tastatur eingegebenen Wert gesetzt. Sobald die Eingabe abgeschlossen ist, werden alle Lichter ausgeschaltet.

Dokument Validieren <Name> <Zeit>

[0168] Der Befehl „Dokument validieren" übermittelt die Nachricht „Dokument <Name> OK?" an das Endgerät und zeigt sie auf dem LCD-Schirm an. Wenn das Individuum das Dokument durch Drücken der Ja- oder Enter-Taste bestätigt, wird das Dokumentnamens-Register auf <Name> gesetzt. Der <Name> muss ASCII-druckbar sein und darf keine Steuerzeichen sowie davor oder danach keine Leerzeichen aufweisen. Während der Aufforderung leuchten die Ja-, Nein- und Stornotasten auf. Sobald die Aufforderung abgeschlossen ist, werden alle Lichter ausgeschaltet.

[0169] Wenn das Individuum „nein" eingibt, wird der Vorgang abgebrochen.

Register Zuweisen <Register> <Text>

[0170] Der Befehl „Register zuweisen" setzt das angegebene allgemeine <Register> auf den Wert <Text>. Dies dient dazu, Informationen wie z. B. den Vertragspartnercode, die Produktinformation usw. zu setzen.

Nachricht Erhalten-Schlüssel

[0171] Der Befehl „Nachricht Erhalten-Schlüssel" bewirkt, dass die BIA einen 56-bit-Zufallsschlüssel erzeugt, um von der Steuerungshardware zur Verschlüsselung eines Nachrichtenkörpers verwendet zu werden, die die Steuervorrichtung der Nachricht hinzufügen möchte. Dieser erzeugte Schlüssel wird in Hexadezimalformat der BIA rückübermittelt (auf dem Gebiet der Erfindung bekannt). Der Nachrichtenschlüssel wird dann dem Biometrik-PIC-Block hinzugefügt.

Nachricht Erstellen <Typ = Identifizierung|Transaktion|Kontozugriff ...>

[0172] Der Befehl „Nachricht erstellen" weist die BIA an, eine Nachricht mit der gesamten von ihr erfassten Information auszugeben. Er überprüft auch, dass alle für diesen spezifischen Nachrichten <Typ> relevanten Register gesetzt wurden. Wenn nicht alle Register gesetzt sind, kehrt die BIA mit einer Fehlermeldung zurück. Die konkrete Software für diesen Befehlssatz bestimmt, welche Nachrichten durch das BIA-Modell gebildet werden können; alle anderen werden abgewiesen.

[0173] Jede Nachricht enthält einen Übertragungscode, der aus dem eindeutigen BIA-Hardware-Identifizierungscode und einer inkrementierenden Folgenummer besteht. Dank des Übertragungscodes kann das DPC die sendende BIA identifizieren und Angriffe mittels erneuter Vorlagen detektieren.

[0174] Die BIA verwendet das DUKPT-Schlüsselverwaltungssystem, um den Biometrik-PIC-Block-Verschlüsselungs-54-bit-DES-Schlüssel aus der Tabelle zukünftiger Schlüssel auszuwählen. Dieser Schlüssel dient zur Verschlüsselung des Biometrik-PIC-Blocks unter Anwendung von Geheimtextblockverkettung (Cipher Block Chaining, CBC). Darüber hinaus wird auch ein Antwort-DES-Schlüssel wahllos erzeugt und vom DPC verwendet, die Abschnitte der Antwort zu verschlüsseln, die verschlüsselt werden müssen.

[0175] Es ist zu beachten, dass der Antwortschlüssel aus dem Biometrik-PIC-Block-Schlüssel sehr wichtig ist, da jeder Verschlüsselungsschlüssel nur innerhalb seines eigenen Zuständigkeitsbereichs verwendet werden darf. Wenn demnach jemand den Schlüssel ermitteln würde, der den privaten Code codiert, würde dies nicht zur Offenlegung des Biometrik-PIC führen.

[0176] Der Biometrik-PIC-Block besteht aus den folgenden Feldern:
300-Btye-Autorisierungs-Biometrik
4-12-stelliger PIC

56-bit-Antwortschlüssel
[gegebenenfalls 56-bit-Nachrichtenschlüssel]

[0177] Es ist zu beachten, dass der Nachrichtenschlüssel nur vorhanden ist, wenn das Steuerungsendgerät einen Nachrichtenschlüssel für diese Nachricht angefordert hat. Es liegt am Steuerungsendgerät, jeden Nachrichtenkörper, der an der Transaktions-Autorisierungsaufforderung angefügt ist, unter Zuhilfenahme des Nachrichtenschlüssels zu verschlüsseln.

[0178] Sobald die Verschlüsselung abgeschlossen ist, gibt die BIA den Körper der entsprechenden Aufforderungsnachricht aus (z. B. eine Transaktionsautorisierungs-Aufforderungsnachricht); beendet und geschützt wird dies vom Nachrichten-Authentifizierungscode (Message Authentication Code, MAC).

[0179] Das MAC-Feld wird mittels des geheimen 112-bit-DES-Mac-Schlüssels der BIA berechnet und deckt alle Nachrichtenfelder vom ersten bis zum letzten ab. Der MAC versichert dem DPC, dass sich nichts in der Nachricht verändert hat, wodurch diese wirkungsvoll versiegelt wird, während die Klartextfelder weiterhin durch das Steuerungsendgerät kontrolliert werden können.

[0180] Wen der Befehl „Nachricht erstellen" ausgeführt ist, sendet die BIA die Nachricht „Ich spreche mit dem DPC" an das Endgerät und zeigt sie auch auf dem LCD-Schirm an, wodurch man erkennt, dass die Aufforderung erledigt wird.

[0181] Nach Abschluss des Befehls sendet dieser OK und sendet die gesamte gebildete Nachricht zurück.

Antwort Zeigen <verschlüsselte Antwort> <Zeit>

[0182] Der Befehl „Antwort zeige" weist die BIA an, ihren aktuellen Antwortschlüssel dazu zu verwenden, den privaten Code aus dem System zu entschlüsseln.

[0183] Nach der Entschlüsselung ertönt ein Signal, und der private Code wird <Zeit> Sekunden lang auf dem LCD-Schirm angezeigt. Dem Steuerungsendgerät wird von diesem Befehl der entschlüsselte private Code niemals zugesendet.

Privat Validieren <vetschlüsselte Validierung> <Zeit>

[0184] Dieser Befehl wird von einem Endgerät während einer sicheren Netzwerk-Kommunikationssitzung dazu verwendet, das Individuum zu bitten, eine Nachricht aus einer externen Quelle zu validieren. Die Nachricht wird in zwei Teilen verschlüsselt übermittelt – dem Abfrage-Teil und dem Antwort-Teil.

[0185] Nach Erhalt des Befehls „privat validieren" zeigt die BIA den Text der Abfrage-Nachricht (z. B. als „OK <Abfrage>?") auf dem LCD-Schirm an, sendet sie aber nicht an das Endgerät. Wenn das Individuum die Abfrage validiert, wird die Antwort durch die BIA unter Verwendung des Schlüssels für private Sitzungen verschlüsselt und gemeinsam mit dem OK-Antwortcode an das Endgerät zurückgeschickt. Wenn das Individuum die Abfrage nicht validiert, reagiert die BIA mit einem „fehlgeschlagenen" Antwortcode und mit dem Text „Vorgang auf Ihren Wunsch abgebrochen", der auf dem LCD-Schirm angezeigt wird.

[0186] Es ist zu beachten, dass das Endgerät niemals den Klartext des Abfrage- oder Antwort-Teils zu sehen bekommt.

Zurücksetzen

[0187] Der Befehl „Zurücksetzen" weist die BIA an, alle temporären Register, den LCD-Schirm, alle temporären Schlüsselregister zu löschen und die noch eingeschalteten Tastenfeldlichter auszuschalten.

PIC Setzen <Wert>

[0188] Diese Befehl weist dem PIC-Register der BIA den <Wert> zu.

[0189] Es ist zu beachten, dass es ein potenzielles Sicherheitsrisiko darstellt, wenn eine nicht gesicherte Vorrichtung den PIC bereitstellt, da nicht gesicherte Geräte gegenüber Abhören oder Austausch viel anfälliger sind.

Kontoindexcode Setzen <Wert>

[0190] Dieser Befehl weist dem Kontoindexcode-Register der BIA den <Wert> zu.

[0191] Es ist zu beachten, dass es ein potenzielles Sicherheitsrisiko darstellt, wenn eine nicht gesicherte Vorrichtung den Kontoindexcode bereitstellt, da nicht gesicherte Geräte gegenüber Abhören oder Austausch viel anfälliger sind.

Titelindexcode Setzen <Wert>

[0192] Dieser Befehl weist dem Titelindexcode-Register der BIA den <Wert> zu.

[0193] Es ist zu beachten, dass es ein potenzielles Sicherheitsrisiko darstellt, wenn eine nicht gesicherte Vorrichtung den Titelindexcode bereitstellt, da nicht gesicherte Geräte gegenüber Abhören oder Austausch viel anfälliger sind.

Betrag Setzen <Wert>

[0194] Dieser Befehl weist dem Betragsregister der BIA den <Wert> zu.

Antwort Entschlüsseln <verschlüsselte Antwortnachricht>

[0195] Der Befehl „Antwort entschlüsseln" weist die BIA an, ihren aktuellen Antwortschlüssel zu benutzen, um den verschlüsselten Abschnitt der Antwortnachricht zu entschlüsseln. Sobald die Antwort entschlüsselt ist, wird sie an die Steuerungsvorrichtung zurückgeschickt, um vermutlich auf dem LED-Schirm des Geldausgabeautomaten angezeigt zu werden.

[0196] Es ist zu beachten, dass das Vorsehen dieser Entschlüsselungsfähigkeit ein Sicherheitsproblem darstellt, da das Endgerät – sobald Klartext die BIA verlässt – damit machen kann, was es will.

1.2.2. BIA-Software: Supportbibliotheken

[0197] Die BIA-Software wird durch verschiedene Softwarebibliotheken unterstützt. Einige von ihnen sind standardmäßige, allgemein verfügbare Bibliotheken, doch einige stellen im Zusammenhang mit der BIA besondere Anforderungen.

1.2.2.1. Zufallszahlengenerator

[0198] Da die BIA unablässig Zufalls-DES-Schlüssel zur Verwendung bei der Verschlüsselung des Nachrichtenkörpers und der Nachrichtenantwort auswählt, ist es wichtig, dass die ausgewählten Schlüssel unvorhersagbare Schlüssel sind. Wenn der Zufallszahlengenerator auf der Tageszeit oder einem anderen von außen vorhersagbaren Mechanismus basiert, kann ein Widersacher, der den Algorithmus kennt, die Verschlüsselungsschlüssel viel leichter erraten. Um die Sicherheit der in der BIA angewendeten Verschlüsselungstechniken zu gewährleisten, nimmt man an, dass sowohl der Zufallszahlengenerator-Algorithmus als auch die Verschlüsselungsalgorithmen jeweils öffentlich bekannt sind.

[0199] Ein Standard-Zufallszahlenalgorithmus zur Erzeugung von DES-Schlüsseln ist in ANSI X9.7, Anhang C definiert (auf dem Gebiet der Erfindung bekannt).

1.2.2.2. DSP-Biometrik-Codieralgorithmen

[0200] Der Biometrik-Codieralgorithmus ist ein priprietärer Algorithmus zur Lokalisierung der Details, die durch Enden kleiner Erhebungen und Gabelungen auf menschlichen Fingerspitzen gebildet werden. Eine vollständige Liste der Details ist im DPC zu Kontrollzwecken gespeichert, während nur ein Teil der Liste vom Algorithmus benötigt wird, wenn er einen Vergleich zwischen einem Identifizierungskandidaten und einem registrierten Individuum zieht.

[0201] Während der biometrischen Registrierung und Identifizierung stellt der Codieralgorithmus sicher, dass ausreichend Details vor der Beendigung des biometrischen Eingabeschritts gesammelt wurden.

1.2.2.3. Betriebssystem und Gerätetreiber

[0202] Die BIA ist eine Echtzeit-Computerumgebung und erfordert daher ein eingebettetes Echtzeit-Betriebssystem. Das Betriebssystem ist dafür verantwortlich, Unterbrechungen in Geräten zu unterbinden und Aufgaben zeitlich einzuteilen.

[0203] Jeder Gerätetreiber ist für die Schnittstelle zwischen dem Betriebssystem und der spezifischen Hardware verantwortlich, z. B. der PIC-Feld-Treiber oder der CCD-Scanner-Treiber. Die Hardware ist die Quelle für Ereignisse wie „PIC-Feldtaste gedrückt" oder „CCD-Scanner-Abtastvorgang abgeschlossen". Der Gerätetreiber kümmert sich um solche Unterbrechungen, interpretiert die Ereignisse und ergreift dann die entsprechenden Maßnahmen.

1.2.2.4. DES-Verschlüsselungsbibliothek

[0204] Es gibt eine Reihe von öffentlich erhältlichen DES-Implementierungen. Die DES-Implementierungen sorgen für geheime Schlüssel-basierte Verschlüsselung von Klartext in verschlüsselten Text und für Entschlüsselung von verschlüsseltem Text in Klartext unter Verwendung von 56-bit-Geheimschlüsseln.

1.2.2.5. Public-Key-Verschlüsselungsbibliothek

[0205] Public-Key-Verschlüsselungs-Supportbibliotheken sind bei einigen Public-Key-Partnern, den Inhabern der RSA-Public-Key-Patente, erhältlich (auf dem Gebiet der Erfindung bekannt). Public-Key-Kryptosysteme sind asymmetrische Verschlüsselungssysteme, mithilfe derer Kommunikation ohne kostspieligen Austausch geheimer Schlüssel stattfinden kann. Um ein Public-Key-Verschlüsselungssystem zu verwenden, dient ein öffentlicher Schlüssel dazu, einen DES-Schlüssel zu verschlüsseln, der dann seinerseits dazu dient, eine Nachricht zu verschlüsseln. Die BIA bedient sich der Public-Key-Kryptosysteme, um für sicheren Austausch von geheimen Schlüsseln zu sorgen.

[0206] Leider sind Public-Key-Systeme deutlich weniger erprobt als Systeme mit Geheimschlüsseln, und infolge davon ist das Vertrauen in solche Algorithmen weniger hoch. Die Erfindung bedient sich daher zum Zwecke der Kommunikationssicherheit und des Kurzzeitaustauschs von Akkreditiven der Public-Key-Kryptographie und nicht der Langzeitspeicherung von Geheimschlüsseln. Sowohl das Individuum, d. h. der Endbenutzer, als auch die Bank werden vom DPC identifiziert, um ein Netzwerk-Akkreditiv zu schaffen. Zum Netzwerk-Akkreditiv zählen die Identifizierung des Endbenutzers sowie der Verbindungskontext (d. h. die TCP/IP-Quellen- und Zielanschlüsse).

1.2.2.6. DUKPT-Schlüsselverwaltungsbibliothek

[0207] Die DUKPT-Verwaltungsbibliothek (DUKPT, derived unique key per transaction key = abgeleiteter eindeutiger Schlüssel pro Transaktionsschlüssel) wird dazu verwendet, zukünftige DES-Schlüssel anhand eines Anfangsschlüssels und einer Nachrichtenfolgenummer zu schaffen. Die zukünftigen Schlüssel sind in einer Tabelle für zukünftige Schlüssel gespeichert. Sobald ein bestimmter Schlüssel verwendet wird, wird er aus der Tabelle gelöscht. Die Anfangsschlüssel werden nur zur Erzeugung der ersten Tabelle für zukünftige Schlüssel verwendet. Daher wird der Anfangsschlüssel von der BIA nicht gespeichert.

[0208] Die Verwendung von DUKPT soll einen Schlüssel-Verwaltungsmechanismus bilden, der einen unterschiedlichen DES-Schlüssel für jede Transaktion bereitstellt, ohne die Spur des Anfangsschlüssels zu hinterlassen. Die Folge davon ist, dass selbst eine erfolgreiche Entwendung und Analyse einer bestimmten Tabelle für zukünftige Schlüssel nicht bedeutet, dass man die bereits gesendeten Nachrichten zu Gesicht bekommt – ein sehr wichtiges Merkmal, wenn die Lebensdauer der übertragenen Informationen Jahrzehnte ist. DUKPT ist in ANSI X9.24 ausführlich spezifiziert (auf dem Gebiet der Erfindung bekannt).

[0209] DUKPT wurde ursprünglich entwickelt, um PIC-Verschlüsselungsmechanismen für Kontokartentransaktionen zu unterstützen. In dieser Umgebung war es entscheidend, alle Transaktionen zu schützen. Nehmen wir nun an, ein Krimineller zeichnet verschlüsselte Transaktionen über den Zeitraum von sechs Monaten auf und gelangt dann an den Verschlüsselungscode aus dem PIC-Feld, den er erfolgreich extrahiert. Der Kriminelle könnte dann eine neue gefälschte Kontokarte für jede Nachricht, die im Lauf dieser sechs Monate übermittelt wurde, herstellen. Gemäß DUKPT jedoch könnten der Diebstahl und die Analyse des Kriminellen nicht dazu führen, dass er vorherige Nachrichten entschlüsselt (obwohl neue Nachrichten trotzdem entschlüsselt werden können, wenn der Kriminelle nach der Analyse das PIC-Feld ersetzt).

[0210] Im Falle des Biometrik-IC stößt der Kriminelle auf noch größere Schwierigkeiten, und selbst wenn die Nachrichten entschlüsselt sind, ist die Umwandlung eines digitalen Biometrik-PICS in einen physikalischen Fingerabdruck viel schwieriger als die Umwandlung eines Kontonummer-PIC in eine Plastikkarte; dies ist eine der großen Vorzüge des Systems ohne Token.

[0211] Wenn allerdings ein Krimineller entschlüsseln kann, kann er auch verschlüsseln, was ihm ermöglichen würde, einen Biometrik-PIC in das System einzugeben, um eine betrügerische Transaktion zu autorisieren. Dies ist zwar schwierig, aber am besten ist es, die dem Kriminellen zur Verfügung stehenden Optionen so weit wie möglich einzuengen, d. h. DUKPT zu verwenden.

1.3. BIA-Software-Befehlssätze

1.3.1. BIA-Software: Befehlssatz für den Einzelhandel

[0212] Die BIA/Einzelhandelssoftware-Schnittstelle exportiert eine Schnittstelle, dank derer bestimmte Kassen-Endgeräte mit dem System interagieren können.

[0213] Die BIA/Einzelhandels-Schnittstelle ist ausgebildet, die folgenden Vorgänge des Endgeräts zu unterstützen:

Transaktionsautorisierung

[0214] Um diese Vorgänge zu implementieren, bietet die BIA/Einzelhandels-Software den folgenden Befehlssatz:
Sprache setzen <Sprache-Name>
Biometrische Daten erhalten <Zeit>
PIC erhalten <Zeit>
Register zuweisen <Register> <Wert>
Kontoindexcode erhalten <Zeit>
Betrag validieren <Betrag> <Zeit>
Betrag eingeben <Zeit>
Nachricht erstellen <Typ>
Antwort zeigen <verschlüsselte Antwort> <Zeit>
Zurücksetzen

1.3.2. BIA-Software: CATV-Befehlssatz (integrierte Fernbedienung)

[0215] Die BIA/CATV-Software-Schnittstelle exportiert einen Befehlssatz, mit dem mit einer Telefon/CATV-BIA integrierte Endgeräte mit dem System interagieren können. Der folgende Vorgang wird unterstützt:
Fern-Transaktionsautorisierung

[0216] Um diesen Vorgang zu implementieren, bietet BIA/CATV den folgenden Befehlssatz:
Biometrische Daten erhalten <Zeit>
PIC setzen <Text>
Register zuweisen <Register> <Text>
Kontoindexcode setzen <Text>
Nachricht erstellen <Typ>
Antwort entschlüsseln <verschlüsselte Antwortnachricht>
Rücksetzen

1.3.3. BIA-Software: Integrierter Fax-Befehlssatz

[0217] Die BIA/Fax-Software-Schnittstelle exportiert einen Befehlssatz, mit dem mit einer Fax-BIA integrierte Endgeräte mit dem System interagieren können. Die folgenden Vorgänge werden unterstützt:
Sichere Faxvorlage
Sichere Faxdaten
Sichere Faxverfolgung
Sichere Faxabrufung
Sichere Faxabweisung

Sichere Faxarchivierung
Sichere Annahme des Faxvertrags
Sichere Abweisung des Faxvertrags
Abruf archivierter elektronischer Dokumente

[0218] Um diese Vorgänge zu implementieren, bietet BIA/Fax den folgenden Befehlssatz:
Biometrische Daten erhalten <Zeit>
PIC setzen <Text>
Titelindexcode setzen <Text>
Register zuweisen <Register> <Wert>
Nachrichtenschlüssel erhalten
Nachricht erstellen <Typ>
Antwort entschlüsseln <verschlüsselte Antwortnachricht>
Rücksetzen

1.3.4. BIA-Software: Registrierungs-Befehlssatz

[0219] Die BIA/Reg-Software-Schnittstelle exportiert eine Schnittstelle, dank derer nicht spezialisierte Computer mit dem System interagieren können, um Individuen zu identifizieren und zu registrieren. Die folgenden Vorgänge werden unterstützt:
Individuelle Identifizierung
Biometrische Registrierung

[0220] Um diese Vorgänge zu unterstützen, bietet BIA/Reg den folgenden Befehlssatz:
Sprache setzen <Sprache-Name>
Biometrische Daten erhalten <Zeit> [primär|sekundär]
PIC erhalten <Zeit>
Register zuweisen <Register> <Text>
Nachrichtenschlüssel erhalten
Nachricht erstellen <Typ>
Antwort zeigen <verschlüsselte Antwort> <Zeit>
Rücksetzen

1.3.5. BIA-Software: PC-Befehlssatz

[0221] Die BIA/PC-Software-Schnittstelle exportiert einen Befehlssatz, der es nicht spezialisierten Computern ermöglicht, elektronische Dokumente zu senden, zu empfangen und zu signieren, Transaktionen über das Netzwerk durchzuführen, und biometrisch abgeleitete Akkreditive an Netzwerkpositionen zu übermitteln. Es werden die folgenden Vorgänge unterstützt:
Vorlage elektronischer Dokumente
Daten elektronischer Dokumente
Verfolgung elektronischer Dokumente
Abruf elektronischer Dokumente
Abweisung elektronischer Dokumente
Archivieren elektronischer Dokumente
Abruf archivierter elektronischer Dokumente
Vorlage elektronischer Signaturen
Überprüfung elektronischer Signaturen
Fern-Transaktionsautorisierung
Netzwerk-Akkreditiv
Gesicherte Verbindung

[0222] Um diese Vorgänge unterstützen zu können, bietet PIA/PC den folgenden Befehlssatz:
Sprache setzen <Sprache-Name>
Biometrische Daten erhalten <Zeit>
PIC erhalten <Zeit>
Kontoindexcode erhalten <Zeit>
Betrag validieren <Betrag> <Zeit>
Betrag eingeben <Zeit>
Dokument validieren <Name> <Zeit>

Register zuweisen <Register> <Text>
Nachrichtenschlüssel erhalten
Nachricht erstellen <Typ>
Antwort zeigen <verschlüsselte Antwort> <Zeit>
Privat validieren <verschlüsselte Validierung> <Zeit>
Rücksetzen

1.3.6. BIA-Software-Aussteller-Befehlssatz

[0223] Die BIA/Iss-Software exportiert eine Schnittstelle, mit der nicht spezialisierte Computer mit dem System interagieren können, um Stapeländerungs-Aufforderungen zu authentifizieren und vorzulegen. Es wird der folgende Vorgang unterstützt:
Aussteller-Batch

[0224] Um diesen Vorgang zu implementieren, bietet BIA/Iss den folgenden Befehlssatz:
Sprache setzen <Sprache-Name>
Biometrische Daten erhalten <Zeit> [primär|sekundär]
PIC erhalten <Zeit>
Register zuweisen <Register> <Wert>
Nachrichtenschlüssel erhalten
Nachricht erstellen <Typ>
Antwort zeigen <verschlüsselte Antwort> <Zeit>
Rücksetzen

1.3.7. BIA-Software: Interner Befehlssatz

[0225] Die BIA/Int-Software exportiert einen Befehlssatz, mit dem nicht spezialisierte Computer mit dem System interagieren können, um Individuen zu identifizieren. Es wird der folgende Vorgang unterstützt:
Individuelle Identifizierung

[0226] Um diesen Vorgang implementieren zu können, bietet BIA/Int den folgenden Befehlssatz:
Sprache setzen <Sprache-Name>
Biometrische Daten erhalten <Zeit>
PIC erhalten <Zeit>
Register zuweisen <Register> <Wert>
Nachrichtenschlüssel erhalten
Nachricht erstellen <Typ>
Antwort zeigen <verschlüsselte Antwort> <Zeit>
Rücksetzen

1.3.8. BIA-Software: Geldausgabeautomat-Befehlssatz (ATM-Befehlssatz)

[0227] Die BIA/ATM-Software-Schnittstelle exportiert einen Befehlssatz, mit dem Geldausgabeautomaten Individuen erkennen können. Es wird der folgende Vorgang unterstützt:
Kontozugriff

[0228] Um diesen Vorgang zu implementieren, bietet BIA/ATM den folgenden Befehlssatz:
Biometrische Daten erhalten <Zeit>
PIC setzen <Text>
Kontoindexcode setzen <Text>
Register zuweisen <Register> <Wert>
Nachricht erstellen <Typ>
Antwort entschlüsseln <verschlüsselte Antwortnachricht>
Rücksetzen

1.4. Endgeräte

1.4.1. Einführung

[0229] Das Endgerät ist die Vorrichtung, die die BIA steuert und sie über eine Modem-, X.25- oder Internet-

verbindung mit dem DPC verbindet; diese Verfahren sind auf dem Gebiet der Erfindung allgemein bekannt. Endgeräte weisen unterschiedliche Formen und Größen auf und erfordern verschiedene Versionen der BIA, um ihre Aufgaben erledigen zu können. Jedes elektronische Gerät, das Befehle ausgibt und Ergebnisse aus der BIA erhält, kann ein Endgerät sein.

[0230] Einige Endgeräte sind Anwendungsprogramme, die auf einem nicht spezialisierten Mikrocomputer ablaufen, während andere Endgeräte Kombinationen spezieller Hard- und Software sind.

[0231] Zwar ist das Endgerät für das Funktionieren des Systems insgesamt von entscheidender Bedeutung, doch setzt das System selbst überhaupt kein Vertrauen in das Endgerät.

[0232] Wenn ein Endgerät dem System Informationen zukommen lässt, validiert das System diese, indem es sie entweder dem Individuum zwecks Bestätigung vorlegt oder indem es sie mit anderen zuvor registrierten Informationen vergleicht und überprüft.

[0233] Endgeräte können zwar einige Teile der BIA-Nachrichten lesen, um zu bestätigen, dass die Daten von der BIA richtig verarbeitet wurden, doch Endgeräte können keine biometrischen Identifizierungsinformationen, z. B. biometrische Daten, den PIC, Verschlüsselungsschlüssel oder Kontoindexcodes, lesen.

[0234] Spezifische BIAs exportieren Sicherheitsfunktionalität an das Endgerät, z. B. PIC-Eingabe und Anzeige von privatem Code. In der Folge werden derartige Vorrichtungen als etwas weniger sicher betrachtet als ihr vollkommen in sich geschlossenes Gegenstück, weshalb ihre Sicherheitsbewertung auch niedriger ausfällt.

[0235] Es gibt unterschiedliche Endgerätetypen, die jeweils mit einem spezifischen BIA-Modelltyp verbunden sind. Es folgt eine kurze Beschreibung von Endgerätetypen.

Geldausgabeautomat (ATM, Automated Teller Machinery)

[0236] Integrierter BIA/ATM mit ATM-Softwarepaket stellt Biometrik-PIC-Zugriff auf Geldausgabeautomaten bereit.

BRT (biometrisches Registrierungsendgerät, Biometric Registration Terminal)

[0237] Standard-BIA mit Registrierungssoftware-Paket, angeschlossen an einen Mikrocomputer, gibt Banken die Möglichkeit, neue Individuen im System sowie ihre Finanzkonten und andere persönlichen Informationen zu registrieren.

CET (Endgerät für zertifizierte E-Mails, Certified Email Terminal)

[0238] Standard-BIA mit PC-Softwarepaket, angeschlossen an einen Mikrocomputer, gibt Individuen die Möglichkeit, zertifizierte E-Mail-Nachrichten zu senden, zu empfangen, zu archivieren, abzuweisen und zu verfolgen.

CPT (Kabel-TV-Kassenendgerät, Cable-TV Point of Sale Terminal)

[0239] BIA/CATV mit CATV-Softwarepaket, angeschlossen an CATV-Breitband, ermöglicht es Individuen mit Biometrik-Fernsehfernbedienungen, Einkäufe über das Fernsehen (Television Shopping) zu tätigen.

CST (Kundendienstendgerät, Customer Service Terminal)

[0240] Standard-BIA mit internem Softwarepaket, angeschlossen an ein Mikrocomputersystem, autorisiert Mitarbeiter, Kundendienst-Datenbankabfragen zu tätigen.

EST (Endgerät für elektronische Signaturen, Electronic Signature Terminal)

[0241] Standard-BIA mit PC-Softwarepaket, angeschlossen an einen Mikrocomputer, ermöglicht es Individuen, elektronische Signaturen auf Dokumenten zu konstruieren und zu verifizieren.

IPT (Internet-Kassenendgerät, Internet Point of Sale Terminal)

[0242] Standard-BIA mit PC-Softwarepaket, angeschlossen an einen Mikrocomputer, ermöglicht es Individuen, mithilfe von Internetverbindungen Produkte von einem Händler zu kaufen, der an das Internet angeschlossen ist.

IT (Ausstellerendgerät, Issuer Terminal)

[0243] Standard-BIA mit PC-Softwarepaket, angeschlossen an einen Mikrocomputer, bietet Banken die Möglichkeit, Änderungs-Batches von Finanzkonten an das DPC zu schicken.

ITT (Internetbankschalter-Endgerät, Internet Teller Terminal)

[0244] Standard-BIA mit PC-Softwarepaket, angeschlossen an einem Mikrocomputer mit Internetverbindung, bietet Individuen die Möglichkeit, Transaktionen mit ihrer Lieblings-Internetbank durchzuführen.

PPT (Telefon-Kassenendgerät, Phone Point of Sale Terminal)

[0245] BIA/CATV mit CATV-Sofwarepaket, integriert mit einem Telefon, bietet Individuen die Möglichkeit, Transaktionen über Telefonleitung zu autorisieren.

RPT (Einzelhandels-Kassenendgerät, Retail Point of Sale Terminal)

[0246] Standard-BIA mit Einzelhandelssoftware, angeschlossen an ein X.25-Netzwerk oder unter Verwendung eines Modems, erlaubt es Individuen, Artikel mittels Transaktionsautorisierungen in einem Geschäft zu kaufen.

SFT (Endgerät für sichere Faxnachrichten, Secure Fax Terminal)

[0247] BIA/catv mit Fax-Softwarepaket, integriert mit einem Faxgerät, bietet Individuen die Möglichkeit, gesicherte Faxnachrichten zu senden, zu empfangen, abzuweisen, zu archivieren und zu verfolgen.

1.4.2. Endgerät: RPT

1.4.2.1. Zweck

[0248] Zweck des RPT ist es, Individuen die Möglichkeit zu geben, Artikel in einem Geschäftslokal zu kaufen, ohne Bargeld, Scheck, Kontokarte oder Kreditkarte zu verwenden.

[0249] Das RPT verwendet BIA/Einzelhandelssoftware, um Finanztransaktionen von einem Individuum zu einem Händler zu autorisieren. Das RPT nimmt Biometrik-PIC-Autorisierungen an und bietet auch standardmäßige Kredit- und Kontokarten-Abtastfunktionen.

[0250] Es ist zu beachten, dass hierin nur biometrische Transaktionen im Detail beschrieben sind. Es ist anzunehmen, dass das RPT auch aus herkömmlichen Kredit- und Kontokarten-Magnetstreifen-Kartenlesegeräten sowie optionalen Smart-Card-Lesegeräten bestehen wird.

1.4.2.2. Konstruktion

[0251] Jedes RPT ist mit dem DPC über ein Modem, eine X.25-Netzwerkverbindung, eine ISDN-Verbindung oder einen ähnlichen Mechanismus verbunden. Das RPT kann auch mit anderen Geräten verbunden sein, z. B. einer elektronischen Kassa, von der es den Betrag der Transaktion und den Händlercode erhält.

[0252] Das RPT besteht aus Folgendem:
- BIA/Einzelhandelssoftware
- einem kostengünstigen Mikroprozessor
- 9,6 kb-Modem/X.25-Netzwerk-Schnittstellen-Hardware
- Händler-Identifizierungscode-Zahl in nichtflüchtigem RAM
- einer seriellen DTC-Schnittstelle zum Anschluss an die BIA
- einem Magnetstreifen-Lesegerät (auf dem Gebiet der Erfindung bekannt)

– ECR-Verbindungsanschluss (ECR = electronic cash register, elektronische Kassa)
– gegebenenfalls einem Smart-Card-Lesegerät (auf dem Gebiet der Erfindung bekannt)

1.4.2.3. Identifizierung

[0253] Es müssen zwei Teilnehmer identifiziert werden, damit das DPC positiv auf eine BIA-Transaktionsautorisierungs-Aufforderung reagiert: das Individuum und der Vertragspartner.

[0254] Das Individuum wird durch den Biometrik-PIC identifiziert, der Händler bzw. Vertragspartner durch das DPC, das den Händlercode in der VAC-Aufzeichnung der BIA mit dem Händlercode vergleicht und überprüft, der an die Transaktionsaufforderung seitens des RPT angefügt ist.

1.4.2.4. Funktionsweise

[0255] Zunächst gibt der Händler den Wert der Transaktion in seine elektronische Kassa ein. Dann gibt das Individuum seinen Biometrik-PIC und seinen Kontoindexcode ein und bestätigt den Betrag. Das RPT fügt danach die Produktinformation und den Händlercode an die BIA an, weist die BIA an, die Transaktion zu erstellen und schickt die Transaktion anschließend über die Netzwerkverbindung (Modem, X.25 usw.) an das DPC.

[0256] Wenn das DPC diese Nachricht empfängt, validiert es den Biometrik-PIC, erhält die Kontonummer unter Verwendung des Indexcodes und überprüft den Händlercode in der Nachricht mit dem registrierten Besitzer der BIA. Wenn alles kontrolliert ist, bereitet das DPC eine Gutschrift/Lastschrift-Transaktion, um den Austausch durchzuführen. Die Antwort vom Gutschrift/Lastschrift-Netzwerk wird dem privaten Code hinzugefügt, um die Transaktionsantwortnachricht zu erstellen, die das DPC dann an das RPT retourniert. Das RPT überprüft die Antwort, um festzustellen, ob die Autorisierung erfolgreich war oder nicht, und leitet die Antwort dann an die BIA weiter, die den privaten Code des Individuums danach anzeigt, wodurch die Transaktion abgeschlossen ist.

1.4.2.5. Sicherheit

[0257] Nachrichten zwischen dem RPT und dem DPC werden durch Verschlüsselung und MAC-Berechnung anhand der BIA gesichert. Aufgrund des MAC kann das RPT die unverschlüsselten Teile der Nachricht sehen, doch das RPT kann diese nicht verändern. Die Verschlüsselung verhindert, dass der verschlüsselte Teil der Nachricht dem RPT bekannt gegeben wird.

[0258] Jede Einzelhandels-BIA muss bei einem Händler registriert sein. Das trägt dazu bei, BIA-Diebstähle zu verhindern. Da außerdem das RPT den Händlercode an jede Nachricht anfügt, wird der Austausch einer Vertragspartner-BIA durch eine andere BIA durch die im DPC vorgenommene Überprüfung erkannt.

1.4.3. Endgerät: Internet-Kassenendgerät

1.4.3.1. Zweck

[0259] Der Zweck eines IPT besteht darin, Gutschrift- und Lastschrift-Finanztransaktionen von einem Individuum am Computer an einen Händler zu autorisieren, die sich beide im Internet befinden.

[0260] Es ist zu beachten, dass das Internet ein Allzwecknetzwerk darstellt, in dem ein Händler, das DPC und das IPT alle in Echtzeit miteinander verbunden sein können. Dieser Mechanismus funktioniert also in gleicher Weise wie in jedem anderen Allzwecknetzwerk.

1.4.3.2. Konstruktion

[0261] Das IPT besteht aus Folgendem:
– eine BIA/PC
– ein Mikrocomputer
– eine Internet Käufer-Softwareapplikation
– eine Internetverbindung (oder andere Netzwerkverbindung)

1.4.3.3. Identifizierung

[0262] Neben der Identifizierung des Individuums muss das IPT auch den an einem entfernten Ort befindlichen Händler identifizieren, der im Rahmen der Transaktion der Gegenteilnehmer ist. Der Händler muss auch sowohl das DPC als auch das IPT identifizieren.

[0263] Das Internet-Käufer-Programm speichert den Hostnamen (oder eine andere Form von Netznamen) des Händlers, bei dem der Einkauf stattfindet, um die Identität des Händlers zu verifizieren. Da der Händler alle seine legitimen Internethosts beim DPC registriert, kann das DPC den Händlercode mit jenem vergleichen und überprüfen, der unter diesem Hostnamen gespeichert ist, um so die Händleridentität zu verifizieren.

1.4.3.4. Funktionsweise

[0264] Zunächst wird das IPT über das Internet mit dem Händler verbunden. Sobald eine Verbindung hergestellt ist, sichert das IPT, indem es einen Sitzungsschlüssel (Session Key) generiert und diesen an den Händler schickt. Um sicherzustellen, dass der Session Key vor Offenlegung geschützt ist, wird er mittels Public Key-Verschlüsselung mit dem Public Key des Händlers verschlüsselt. Wenn der Händler diesen verschlüsselten Session Key erhält, entschlüsselt er ihn mit seinem Private Key. Dieser Vorgang wird als Sichern einer Verbindung mittels Public Key-verschlüsselten Geheimschlüssel-Austausch bezeichnet.

[0265] Sobald die Verbindung hergestellt ist, lädt das IPT den Händlercode sowie den Preis und die Produktinformation vom Geschäftslokal herunter. Sobald das Individuum zum Kauf bereit ist, wählt er die von ihm gewünschte Ware aus. Dann gibt das Individuum unter Einsatz von BIA/PC den Biometrik-PIC ein, das IPT sendet den Händlercode, die Produktidentifizierungsinformation und den Betrag an die BIA und weist diese an, eine Ferntransaktions-Autorisierungsaufforderung zu generieren. Dann leitet die IPT die Aufforderung über den sicheren Kanal an den Händler weiter.

[0266] Der Händler ist über die gleiche sichere Verbindung an das DPC angeschlossen, mit der das IPT mit dem Händler verbunden ist, d. h. mittels Public Key-Verschlüsselung zum Versand eines sicheren Session Key. Im Gegensatz zur IPT-Händler-Verbindung jedoch gelten die Händler-DPC-Session Keys einen ganzen Tag lang, nicht nur für die Dauer einer Verbindung.

[0267] Der Händler schafft eine Verbindung zum DPC, wobei er diese mittels des Session Key sichert und die Transaktion zwecks Validierung an das DPC weiterleitet. Das DPC validiert den Biometrik-PIC, vergleicht den in der Aufforderung enthaltenen Händlercode mit dem Händlercode, der unter dem in der Aufforderung übermittelten Hostnamen gespeichert ist, und sendet dann eine Transaktion an das Gutschrift/Lastschrift-Netzwerk. Sobald dieses antwortet, konstruiert das DPC eine Antwortnachricht einschließlich der Gutschrift/Lastschrift-Autorisierung, eines verschlüsselten privaten Codes und der Adresse des Individuums und retourniert diese Nachricht an den Händler.

[0268] Sobald der Händler die Antwort erhält, kopiert er die Postadresse des Individuums aus der Antwort, notiert sich den Autorisierungscode und leitet die Antwortnachricht an das IPT weiter.

[0269] Das IPT übergibt die Antwort an die BIA, die den privaten Code entschlüsselt und ihn auf dem LCD-Schirm anzeigt – das DPC hat somit das Individuum erkannt. Das IPT zeigt auch das Ergebnis der Transaktion, ob es nun erfolgreich war oder nicht.

1.4.3.5. Sicherheit

[0270] Da das System im Allgemeinen annimmt, dass ein feindlich gesinnter Netzteilnehmer Netzwerkverbindungen jederzeit kapern kann, müssen alle Teilnehmer während ihrer in Echtzeit ablaufenden Interaktionen sicher miteinander kommunizieren. Das Hauptproblem ist nicht die Offenlegung von Informationen, sondern das Einfügen oder Umleiten von Nachrichten.

[0271] Das gesamte System der Public Key-Verschlüsselung beruht auf einer vertrauenswürdigen Quelle dieser Public Keys. Diese vertrauenswürdigen Quellen werden als Zertifizierungsstellen bezeichnet, und man kann annehmen, dass eine solche Quelle in der absehbaren Zukunft auch im Internet verfügbar sein wird.

1.4.4. Endgerät: Internetbankschalter-Endgerät

1.4.4.1. Zweck

[0272] Das ITT dient dazu, Individuen für Internet-Banksitzungen zu identifizieren. Das DPC, das Computersystem der Bank und das Individuum sind alle an das Internet angeschlossen.

[0273] Es gibt zwei Hauptaufgaben zu erfüllen. Die erste ist die Bereitstellung eines sicheren Kommunikationskanals vom ITT zur Internetbank. Die zweite ist die Lieferung unanfechtbarer Identitäts-Akkreditive an die Internetbank. Sobald beide Kriterien erfüllt sind, kann das ITT für eine sichere Internet-Banksitzung sorgen. Außerdem dient die Abfrage-Antwort-Verifizierungsfähigkeit der BIA dazu, zusätzliche Sicherheit für alle hohe Geldbeträge umfassenden und/oder außergewöhnlichen Transaktionen zu schaffen.

1.4.4.2. Konstruktion

[0274] Das ITT besteht aus Folgendem:
- ein BIA (Standard-PC-Modell)
- ein Mikrocomputer
- eine Internet Teller-Softwareapplikation
- ein Internetverbindung

[0275] Das ITT akzeptiert die biometrische Identifizierung unter Einsatz von BIA/PC, die an den Mikrocomputer angeschlossen ist, der als Internetendgerät des Individuums dient.

1.4.4.3. Identifizierung

[0276] Sowohl das Individuum als auch die Bank werden vom DPC identifiziert, um ein Netzwerk-Credential vorzulegen. Dazu zählen die Identifizierung des Individuums sowie der Verbindungskontext (d. h. die TCP/IP-Quellen- und Zielanschlüsse).

[0277] Das DPC identifiziert die Bank durch Vergleichen des von der Bank an das ITT gesendeten Codes mit dem Hostnamen der Bank, den das ITT an das DPC übermittelt.

1.4.4.4. Funktionsweise

[0278] Zunächst stellt das ITT eine Verbindung zur Internetbank her, wobei darauf geachtet wird, dass die Bank über die notwendigen Computerressourcen verfügt, um eine neue Sitzung für das Individuum abwickeln zu können. Wenn die Bank über ausreichende Ressourcen verfügt, schickt sie den Bank-Identifizierungscode an das ITT zurück.

[0279] Sobald die Verbindung hergestellt ist, weist das ITT die BIA an, den Biometrik-PIC und den Kontoindexcode vom Individuum zu erhalten. Dann fügt das ITT sowohl den Hostnamen der Bank als auch den Bankcode an. Unter Zuhilfenahme all dieser Informationen wird die BIA dann ersucht, eine Netzwerk-Credential-Aufforderungsnachricht zu erstellen, die das ITT über das Internet an das DPC schickt.

[0280] Wenn das DPC diese Nachricht empfängt, validiert es den Biometrik-PIC, erhält die Kontonummer mittels des Indexcodes und stellt sicher, dass der Bankcode aus der Nachricht mit dem Bankcode übereinstimmt, der unter dem Hostnamen der Bank in der Datenbank des an einem entfernten Ort befindlichen Händlers gespeichert ist. Das DPC stellt auch sicher, dass die vom Indexcode zurückgeschickte Kontonummer ebenso der Bank gehört. Wenn alles überprüft ist, erstellt das DPC ein Netzwerk-Akkreditiv unter Verwendung der Kontoidentifizierung des Individuums, der Tageszeit und des Bankcodes bzw. der Bankleitzahl. Das DPC signiert dieses Akkreditiv mittels Public Key-Verschlüsselung und des Private Key des DPC. Das DPC ruft den Public Key der Bank und den privaten Code des Individuums auf und erstellt mit dem Akkreditiv die Netzwerk-Credential-Antwortnachricht. Die Antwortnachricht wird mittels des BIA-Antwortschlüssels verschlüsselt und dann an das ITT zurückgesendet.

[0281] Wenn das ITT die Antwort erhält, übergibt es die Antwortnachricht an die BIA. Die BIA entschlüsselt den privaten Code des Individuums und zeigt ihn danach auf dem LCD-Schirm an. Der Public Key der Bank ist im Public Key-Register gespeichert. Zwei Random Session Keys werden von der BIA erzeugt. Der erste Schlüssel, der „Schlüssel für gemeinsame Sitzungen" (Shared Session Key), wird dem ITT im Klartext offen

gelegt. Das ITT sichert mithilfe dieses Shared Session Key die Verbindung mit der Bank.

[0282] Der andere Session Key, der „Schlüssel für private Sitzungen" (Private Session Key), wird nicht mit dem ITT geteilt. Er wird für den Challenge-Response-Mechanismus der BIA verwendet, einen Mechanismus, der es der Bank erlaubt, spezifische Validierung für Nicht-Routinetransaktionen direkt vom Individuum zu erhalten, ohne das (nicht vertrauenswürdige) ITT zu involvieren.

[0283] Nach Erhalt des Shared Session Key bittet das ITT die BIA, eine Aufforderungsnachricht für eine gesicherte Verbindung zu erstellen; sie umfasst beide Session Keys und das Netzwerk-Akkreditiv, und alles ist mit dem Public Key der Bank verschlüsselt. Das ITT schickt dann die Aufforderungsnachricht für eine gesicherte Verbindung an die Bank.

[0284] Wenn die Bank die Aufforderungsnachricht erhält, entschlüsselt sie die Nachricht mit ihrem eigenen Private Key. Dann entschlüsselt sie das Netzwerk-Credential mit dem Public Key des DPC. Wenn das Netzwerk-Credential gültig und nicht abgelaufen ist (ein Credential läuft nach einigen Minuten ab), wird das Individuum autorisiert, und die Konversation wird unter Verwendung des Session Key zur Gewährleistung von Sicherheit fortgesetzt.

[0285] Wenn das Individuum Nicht-Routinetransaktionen oder Transaktionen mit hohen Geldbeträgen durchführt, bittet die Bank das Individuum möglicherweise, diese Transaktionen zwecks höherer Sicherheit zu bestätigen. Zu diesem Zweck sendet die Bank eine mit dem Private Session Key verschlüsselte Abfrage-Antwort-Nachricht and das ITT, das diese Challenge-Response-Nachricht and die BIA weiterleitet. Die BIA entschlüsselt die Nachricht, zeigt die Abfrage (üblicherweise in Form von „Überweisung von $ 2031,23 an Rick Adams OK?"), und wenn das Individuum durch Drücken des OK-Knopfs diese Frage bestätigt, verschlüsselt die BIA die Antwort erneut mit dem Private Session Key und sendet diese Nachricht an das ITT, das sie an die Bank weiterleitet, wodurch die Transaktion validiert wird.

1.4.4.5. Sicherheit

[0286] Das System macht sich Public Key-Kryptographie zunutze, um sowohl Akkreditive zu präsentieren als auch für sichere Kommunikation zwischen dem ITT und der Bank zu sorgen.

[0287] Damit dieser Mechanismus richtig funktioniert, muss die Bank den Public Key des DPC kennen, und das DPC muss den Public Key der Bank kennen. Es ist in Bezug auf die Systemsicherheit entscheidend, dass beide Teilnehmer die jeweiligen Public Keys vor unautorisierter Modifikation schützen. Es ist zu beachten, dass jeder öffentliche Schlüssel lesen kann, dass aber nicht jeder sie modifizieren kann.

[0288] Natürlich müssen alle Sitzungs- oder Geheimschlüssel vor unerwünschter Beobachtung geschützt werden, wobei Geheimschlüssel nach Beendigung der Sitzung zerstört werden müssen.

[0289] Der zusätzliche Validierungsschritt für Nicht-Routinetransaktionen ist notwendig, da es relativ schwierig ist, PC-Anwendungen im Internet vor Viren, Hackern und der Unwissenheit von Benutzern zu sichern. Die Banken sollten wahrscheinlich die für ITTs möglichen Routine-Geldüberweisungen nur auf Geldüberweisungen an bekannte Institutionen wie z. B. Energieerzeugungsunternehmen, große Kreditkartenverkäufer usw. einschränken.

1.4.5. Endgerät: Endgerät für elektronische Signaturen

1.4.5.1. Zweck

[0290] Das EST wird von Individuen dazu benutzt, für elektronische Dokumente fälschungssichere elektronische Signaturen zu generieren. Das EST ermöglicht es Individuen entweder, elektronische Dokumente zu signieren, oder verifiziert elektronische Signaturen, die sich bereits in diesen Dokumenten befinden.

1.4.5.2. Konstruktion

[0291] Das EST besteht aus Folgendem:
- eine BIA/PC
- ein Mikrocomputer
- ein Message Digest-Codieralgorithmus (kryptographische Prüfsummen)

– eine Modem-, X.25- oder Internetverbindung
– ein Softwareapplikation für elektronische Signaturen

[0292] Das EST verwendet an einen Mikrocomputer angefügte BIA/PC, wobei die Ereignisse durch eine Softwareapplikation für elektronische Signaturen gesteuert werden.

1.4.5.3. Identifizierung

[0293] Um eine digitale Signatur ohne Public/Private Key-Token zu erstellen, müssen drei Dinge berücksichtigt werden. Erstens muss das zu signierende Dokument eindeutig identifiziert, zweitens die Tageszeit aufgezeichnet und drittens das die Signatur durchführende Individuum identifiziert sein. Dadurch entsteht eine Verbindung zwischen dem Dokument, dem Individuum und der Zeit, wodurch eine zu einem eindeutigen Zeitpunkt erstellte elektronische Signatur entsteht.

1.4.5.4. Funktionsweise

[0294] Zunächst wird das zu signierende Dokument durch einen Message Digest-Codieralgorithmus verarbeitet, der einen Message Digest-Code erstellt. Ein derartiger Algorithmus ist der MD5-Algorithmus von RSA, der auf dem Gebiet der Erfindung allgemein bekannt ist. Es ist die Beschaffenheit von Message Digest-Algorithmen, dass sie solcherart spezifisch ausgebildet sind, dass es fast unmöglich ist, ein anderes Dokument zu präsentieren, das den gleichen Message Digest-Code generiert.

[0295] Dann gibt das Individuum seinen Biometrik-PIC unter Zuhilfenahme der BIA ein, der Message Digest-Code wird an die BIA übergeben, der Name des Dokuments wird hinzugefügt, und die resultierende Aufforderungsnachricht zur Erstellung einer digitalen Signatur wird zwecks Autorisierung und Speicherung an das DPC gesendet.

[0296] Wenn das DPC die Aufforderung erhält, führt es eine biometrische Identitätskontrolle durch, und sobald das Individuum verifiziert wurde, werden die Message Digest-Codierung, die biometrische Kontonummer des Individuums, die aktuelle Tageszeit, der Name des Dokuments und die Identifizierung der die Signatur erfassenden BIA erfasst und alle diese Informationen in der Datenbank für elektronische Signaturen (ESD, Electronic Signatures Database) gespeichert. Das DPC konstruiert dann einen Signaturcode-Textstring, der aus der ESD-Eintragnummer, dem Datum, der Tageszeit und dem Namen des Signierenden besteht, und schickt diesen Signaturcode gemeinsam mit dem privaten Code des Individuums zurück an das EST.

[0297] Um eine elektronische Signatur zu kontrollieren, wird das Dokument durch den auf dem Gebiet der Erfindung bekannten MD5-Algorithmus geschickt, und der resultierende Wert wird gemeinsam mit den elektronischen Signaturcodes und dem Biometrik-PIC des anfragenden Individuums an die BIA übergeben; dann wird die Nachricht an das DPC geschickt. Das DPC überprüft jede Signatur auf Gültigkeit und reagiert dementsprechend.

1.4.5.5. Sicherheit

[0298] Die BIA verschlüsselt die Daten betreffend elektronische Signaturen nicht, so dass Dokumenttitel gemeinsam mit spezifischen MD5-Werten in Klartext gesendet werden. Das Gleiche trifft auf Signaturvalidierungen zu.

[0299] Somit können zwar Signaturen nicht gefälscht werden, doch einige der Details (z. B. Dokumentnamen) könnten abgefangen werden.

1.4.6. Endgerät: Endgerät für zertifizierte E-Mails

1.4.6.1. Zweck

[0300] Der Zweck des CET beseht darin, Individuen die Möglichkeit zu geben, elektronische Nachrichten an andere Individuen im System zu versenden, während gleichzeitig der Absender identifiziert, Erhalt und Empfänger verifiziert und die Vertraulichkeit der Nachrichtenübermittlung sichergestellt wird.

[0301] Das CET arbeitet mit BIA/PC, um sowohl den Absender als auch den Empfänger zu identifizieren. Sicherheit wird durch Verschlüsseln der Nachricht, durch Verschlüsseln des Nachrichtenschlüssels mittels der

Absender-BIA während das Hochladens und dann durch Entschlüsseln des Nachrichtenschlüssels mittels der Empfänger-BIA während des Herunterladens geboten.

1.4.6.2. Konstruktion

[0302] Sowohl das Absender- als auch das Empfänger-CET sieht Folgendes vor:
- eine BIA
- einen Mikrocomputer
- eine Modem-, X.25- oder Internetverbindung
- die Fähigkeit des E-Mail-Empfangs
- eine Applikation für zertifizierte E-Mails

[0303] Ein CET ist im Grunde genommen ein Mikrocomputer mit E-Mail-Applikation und Netzwerkverbindung, der die BIA auffordert, Biometrik-PIC-Autorisierungen zu erstellen, damit zertifizierte elektronische Nachrichten gesendet und empfangen werden können.

1.4.6.3. Identifizierung

[0304] Um die Zustellung der Nachricht gewährleisten zu können, müssen sowohl der Absender als auch die Empfänger identifiziert sein.

[0305] Der Absender identifiziert sich mit seinem Biometrik-PIC, wenn er die Nachrichten an das DPC hochlädt. Jeder Empfänger, an den der Absender das Dokument schicken möchte, ist entweder durch seine biometrische Kontoidentifizierungsnummer, durch seine Faxnummer oder durch seine Durchwahl identifiziert. Damit ein Empfänger die Nachricht herunterladen kann, identifiziert er sich mittels seines Biometrik-PIC. Dieses Verfahren ähnelt einem persönlichen Telefonat.

1.4.6.4. Funktionsweise

[0306] Die Zustellung der Nachricht beginnt damit, dass ein Individuum ein Dokument oder eine Nachricht hochlädt und sich mittels seines Biometrik-PIC identifiziert. Das Individuum verifiziert dann den Namen des Dokuments, und die E-Mail-Nachricht wird verschlüsselt und hochgeladen.

[0307] Sobald die Nachricht hochgeladen ist, erhält der Absender einen Nachrichten-Identifizierungscode, mit dem der aktuelle Zustellstatus des den Empfängern übermittelten Dokuments angefordert werden kann.

[0308] Das DPC sendet eine elektronische Nachricht an jeden Empfänger und teilt ihnen mit, wann eine zertifizierte Nachricht eingetroffen ist.

[0309] Sobald der Empfänger die Benachrichtung bekommt, kann er diese Nachricht oder eine Gruppe von Nachrichten nach seinem Gutdünken annehmen oder abweisen, indem er seinen Biometrik-PIC vorlegt und ihn durch das DPC validieren lässt.

[0310] Sobald das Dokument erfolgreich allen Empfängern zugestellt wurde, wird es nach einer vorbestimmten Zeit entfernt, im Allgemeinen nach 24 Stunden. Individuen, die das Dokument sowie Informationen über alle Personen, an die die Nachricht gesendet wurde, archivieren wollen, können vor dem Löschen der Nachricht Aufforderungen zum Archivieren der Nachrichten übermitteln.

1.4.6.5. Sicherheit

[0311] Um dem Sicherheitsaspekt der Übertragung Genüge zu tun, wird das Dokument während seines Versands vor Offenlegung geschützt. Das CET erreicht dies unter Verwendung des durch die BIA erzeugten 56-bit-Nachrichtenschlüssels. Da die BIA für die Verschlüsselung des Nachrichtenschlüssels als Teil des Biometrik-PIC verantwortlich ist, wird der Verschlüsselungsschlüssel zuverlässig und sicher an das DPC übermittelt.

[0312] Wenn ein Individuum die Nachricht herunterlädt, wird der Nachrichtenschlüssel gemeinsam mit dem privaten Code verschlüsselt gesendet, so dass der Empfänger die Nachricht entschlüsseln kann. Es ist zu beachten, dass alle Empfänger diesen Nachrichtenschlüssel besitzen können, da sie alle die gleiche Nachricht erhalten.

[0313] Wie beim ITT müssen Individuen Sorge tragen, ihre CET-Applikationssoftware vor heimlicher und unerlaubter Modifikation zu sichern, da ein modifiziertes CET jedes beliebige Dokument senden kann, sobald das Individuum den Dokumentnamen validiert.

1.4.7. Endgerät: Endgerät für sichere Faxnachrichten

1.4.7.1. Zweck

[0314] Der Zweck des Endgeräts für sichere Faxnachrichten (SFT) besteht darin, Individuen die Möglichkeit zu geben, Faxnachrichten an andere Personen im System zu senden, während der Absender identifiziert, sowohl der Erhalt als auch der Empfänger verifiziert und die Vertraulichkeit der Nachrichtenübermittlung sichergestellt wird.

[0315] Jedes SFT verwendet integrierte BIA/catv, um sowohl den Absender als auch den Empfänger zu identifizieren. Die Kommunikationssicherheit wird durch Verschlüsselung erreicht.

1.4.7.2. Konstruktion

[0316] Sowohl das Sender- als auch das Empfänger-SFT besteht aus Folgendem:
- eine BIA/catv
- ein Faxgerät
- gegebenenfalls ein ISDN-Modem

[0317] Ein SFT ist ein über ein Modem an das DPC angeschlossenes Faxgerät. Das System behandelt Faxe als anderen Typ zertifizierter E-Mails.

1.4.7.3. Identifizierung

[0318] Es gibt für sichere Faxe unterschiedliche Sicherheitsstufen, doch gemäß der sichersten Version wird die Identität des Absenders und aller Empfänger verifiziert.

[0319] Der Absender identifiziert sich mittels seines Biometric-PIC und Titelindexcodes, wenn er seine Nachricht an das DPC sendet. Zum Empfang der Faxnachricht identifiziert sich jeder Empfänger selbst, und dies erfolgt wiederum unter Verwendung seines Biometrik-PIC und Titelindexcodes.

[0320] Außerdem wird der Empfangsstandort durch eine Telefonnummer identifiziert. Diese Telefonnummer ist beim DPC registriert. Für gesicherte vertrauliche Faxnachrichten wird jeder Empfänger mit der Telefonnummer und der Durchwahl identifiziert.

1.4.7.4. Funktionsweise

[0321] Es gibt fünf Grundtypen von Faxnachrichten, die ein SFT schicken kann.

I. Ungesicherte Faxe

[0322] Ungesicherte Faxe entsprechen Standardfaxen. Der Absender gibt die Telefonnummer des Empfängers ein und versendet das Fax. In diesem Fall bleibt der Absender unidentifiziert, und das Fax wird an eine bestimmte Telefonnummer geschickt, wobei man hofft, dass es dem richtigen Empfänger zugestellt wird. Ein SFT markiert die oberste Zeile aller solcher ungesicherter Faxe auffällig mit „UNGESICHERT". Alle von Nicht-SFT-Faxgeräten erhaltene Faxnachrichten sind immer als ungesichert markiert.

II. Absender-gesicherte Faxe

[0323] In einem Absender-gesicherten Fax wählt der Absender im Faxgerät den Modus „Absender-gesichert" aus, gibt seinen Biometrik-PIC und danach seinen Titelindexcode ein. Das Faxgerät stellt danach die Verbindung zum DPC her und übermittelt die Informationen betreffend Biometrik-PIC. Sobald das DPC die Identität des Individuums verifiziert hat, sendet die Person das Fax, indem sie das Dokument in den Faxscanner legt. In diesem Fall wird das Fax an das DPC geschickt, das das Fax digital aufbewahrt. Sobald die gesamte Faxnachricht im DPC eingelangt ist, beginnt dieses, das Fax an jeden Zielort zu verschicken, wobei jede Seite mit dem Namen, Titel und Unternehmen des Absenders sowie mit der Kopfzeile „ABSENDER-GESICHERT"

versehen wird.

III. Gesicherte Faxe

[0324] Bei gesicherten Faxnachrichten wählt der Absender den „gesicherten" Modus im Faxgerät aus, gibt seinen Biometrik-PIC und anschließend seinen Titelindexcode ein und wählt dann die Telefonnummern der Empfänger. Sobald das System die Identität des Absenders und alle Telefonnummern der Empfänger verifiziert hat, sendet die Person das Fax, indem sie das Dokument in den Faxscanner legt. Das Fax wird dann an das DPC verschickt, die es digital aufbewahrt. Sobald die gesamte Faxnachricht im DPC eingetroffen ist, übermittelt dieses ein kleines Deckblatt an den Zielort, auf dem das zu erwartende gesicherte Fax, der Absendertitel und seine Identität sowie die Anzahl der zu erwartenden Seiten wie auch ein Verfolgungscode vermerkt sind. Der Verfolgungscode wird automatisch in den Speicher des Empfängerfaxgeräts eingegeben.

[0325] Um das Fax abzurufen, kann jeder Mitarbeiter des Empfängerunternehmens den „Faxabruf"-Knopf auf seinem Faxgerät betätigen, auswählen, welches zu erwartende Fax er mittels des Verfolgungscodes abrufen möchte, und dann den Biometrik-PIC eingeben. Wenn die Faxnachricht unerwünscht ist, kann das Individuum den „Fax abweisen"-Knopf betätigen, doch er muss sich dafür gegenüber dem System trotzdem identifizieren. Sobald das Fax als unternehmensintern validiert ist, wird es auf das Faxgerät des Empfängers heruntergeladen. Jede Seite ist oben mit dem Vermerk „GESICHERT" sowie der Identität und Titelinformation des Absenders versehen.

IV. Gesicherte vertrauliche Faxe

[0326] Im Falle gesicherter vertraulicher Faxe wählt der Absender in seinem Faxgerät den „gesichert-vertraulich"-Modus, gibt seinen Biometrik-PC, anschließend seinen Titel- und Indexcode und dann die Telefonnummer und Systemnebenstelle jedes Empfängers ein. Sobald das DPC die Absenderidentität und die Telefonnummern und Nebenstellen jedes der Teilnehmer verifiziert hat, sendet die Person das Fax, indem sie das Dokument in den Faxscanner legt. Das Fax wird an das DPC übermittelt, das es digital speichert. Sobald die gesamte Faxnachricht im DPC eingetroffen ist, sendet dieses ein kleines Deckblatt an jeden Zielort, auf dem das zu erwartende gesicherte vertrauliche Fax, der Absendertitel, seine Identität, der Titel und die Identität des Empfängers sowie die Anzahl der zu erwartenden Seiten und ein Verfolgungscode vermerkt sind. Dieser Verfolgungscode wird automatisch in den Speicher des Empfängerfaxgeräts eingegeben. Doch nur das Individuum, das das Fax abruft, ist das Individuum, dessen Durchwahlcode angezeigt ist.

[0327] Dieses Individuum betätigt den „Faxabruf"-Knopf, wählt das abzurufende Fax aus und gibt dann seinen Biometrik-PIC ein. Sobald die Faxnachricht als Empfänger validiert ist, wird sie auf das Faxgerät des Empfängers heruntergeladen. Jede Seite ist oben mit dem Vermerk „GESICHERT-VERTRAULICH" sowie mit dem Absendertitel und Informationen betreffend seine Identität versehen.

V. Gesicherte vertrauliche Vertragsfaxe

[0328] Diese Faxe werden, was die tatsächliche Übermittlung des Fax an den Empfänger betrifft, hinsichtlich ihrer Zustellung an die Empfänger identisch mit den gesicherten vertraulichen Faxnachrichten verarbeitet, außer dass sie als „VERTRAG" anstelle von „GESICHERT-VERTRAULCH" gekennzeichnet sind. Außerdem archiviert das DPC die Vertragsfaxe automatisch. Jeder Empfänger kann den Vertrag durch das SFT nach Erhalt des Vertragsfaxes annehmen oder ablehnen. Mit dieser Option übernimmt das DPC die Rolle eines elektronischen Notars.

[0329] Jedes Fax, das an das System geschickt und dann an den Empfänger weitergeleitet wird, kann an eine beliebige Anzahl an Empfängern gesendet werden, ohne das absendende Faxgerät zu überlasten. Außerdem wird die Verfolgungsnummer jedes gesendeten Faxes in den Speicher des Faxgeräts eingegeben; ein Statusbericht über jedes aktuelle Fax kann im Absenderfaxgerät erstellt werden, indem der „Status"-Knopf betätigt und dann der konkrete Verfolgungscode des aktuellen Faxes ausgewählt wird. Das DPC gibt einen Bericht aus, der sofort an das Absenderfaxgerät geschickt wird, in dem für jeden Empfänger die Zustellungssituation detailliert dargestellt wird.

[0330] Im Fall von gesicherten oder gesicherten-vertraulichen Faxnachrichten besteht die Option, dass entweder der Absender oder einer der Empfänger das Fax für die Zukunft archiviert (zusammen mit Detailinformationen bezüglich des Absenders und der Empfänger). Zu diesem Zweck wird jedes gesicherte Fax über einen bestimmten Zeitraum (d. h. 24 Stunden) nach erfolgreicher Zustellung aufbewahrt. Ein Archivverfolgungs-

code wird bei jeder Archivanfrage an das Individuum zurückgeschickt. Dieser Archivcode dient zum Abruf von Faxen und Faxstatusberichten, die im System archiviert sind.

[0331] Archivierte Faxe werden nach einer bestimmten Zeit (d. h. 24 Stunden) im Nur-Lese-Sekundärspeicher aufbewahrt. Das Abrufen eines archivierten Faxes erfordert das Eingreifen eines Menschen und kann bis zu 24 Stunden in Anspruch nehmen.

1.4.7.5. Sicherheit

[0332] Das SFT-System soll sicherstellen, dass der Empfänger die Identität des Absenders erfährt und dass der Absender erfährt, dass der Empfänger den Erhalt des Dokuments bestätigt hat.

[0333] Um Schutz vor unerlaubtem Abfangen oder unerlaubten Eingriffen in die Kommunikation zwischen dem Absender und dem Empfänger zu bieten, verschlüsselt das Faxendgerät das Fax unter Einsatz der von der BIA bereitgestellten Nachrichtenschlüssel-Funktion. Da die BIA für die Verschlüsselung des Nachrichtenschlüssels als Teil des Biometrik-PIC verantwortlich ist, wird der Verschlüsselungsschlüssel gesichert an das DPC geschickt.

[0334] Wenn ein Individuum ein gesichertes Fax jeden beliebigen Typs erhält, wird der Nachrichtenschlüssel gemeinsam mit dem privaten Code verschlüsselt geschickt, damit der Empfänger die Nachricht entschlüsseln kann. Es ist zu beachten, dass durchaus alle Empfänger diesen Nachrichtenschlüssel besitzen können, da sie alle die gleiche Nachricht erhalten.

1.4.7.6. Anmerkungen

[0335] Das Versenden gesicherter Faxe weist starke Ähnlichkeiten mit dem Verschicken von E-Mails auf, und es kommt auch häufig die gleiche Software dabei zum Einsatz.

[0336] Es ist möglich, Faxendgeräte zu konstruieren, die keine integrierten BIA/Fax-Geräte, sondern einen Anschluss aufweisen, der sich zur Anfügung an externe BIA/PC und Software für die BIA eignet.

1.4.8. Endgerät: Biometrisches Registrierungsendgerät

1.4.8.1. Zweck

[0337] Der Zweck des biometrischen Registrierungsendgeräts (BRT) besteht darin, neue Individuen einschließlich ihres Biometrik-PIC, ihrer Zustelladresse, ihres privaten Codes, ihrer E-Mail-Adressen, einer Liste von Titeln und Titelindexcodes zum Senden und Empfangen elektronischer Nachrichten und Faxe sowie einer Liste von Finanzkonten und Kontoindexcodes, auf die sie zugreifen können (alles mittels ihres Biometrik-PIC), zu registrieren.

[0338] Das Ziel des Registrierungsverfahrens ist die Erfassung persönlicher Informationen über ein Individuum am Standort einer verantwortungsbewussten Stelle, wo diese Informationen validiert werden können. Dazu zählen u. a. Bankfilialen und Personalabteilungen von Unternehmen. Jede teilnehmende verantwortungsbewusste Stelle besitzt ein BRT, das von einer Gruppe von Mitarbeitern verwendet wird, die zur Durchführung von Registrierungen ermächtigt wurden. Jeder Mitarbeiter ist für jedes registrierte Individuum verantwortlich.

1.4.8.2. Konstruktion

[0339] Das BRT besteht aus Folgendem:
- ein Mikrocomputer und Schirm, Tastatur, Maus
- eine BIA/Reg
- ein 9,6 kb-Modem-/X.25-Netzwerkverbindung (auf dem Gebiet der Erfindung bekannt)
- eine Softwareapplikation für biometrische Registrierung

[0340] Das BRT bedient sich für die biometrische Eingabe einer angefügten BIA/Reg und ist über ein 9,6 kb-Modem oder eine X.25-Netzwerkverbindung an das System angeschlossen (auf dem Gebiet der Erfindung bekannt). Biometrische Registrierungsendgeräte befinden sich an physikalisch sicheren Orten wie z. B in Bankfilialen.

1.4.8.3. Identifizierung

[0341] Drei Instanzen müssen identifiziert werden, damit das DPC positiv auf eine BIA/Reg-Registrierungsaufforderung reagiert: der registrierende Mitarbeiter, die Institution und die BIA/Reg. Der Mitarbeiter muss autorisiert worden sein, um Individuen für diese Institution zu registrieren.

[0342] Die Institution und die BIA werden durch Gegenvergleichen des Besitzers der BIA mit dem durch das BRT gesetzten Institutionscode identifiziert. Der Mitarbeiter identifiziert sich gegenüber dem System, indem er nach dem Beginn der Registrierungsanmeldung seinen Biometrik-PIC eingibt.

[0343] Die Institution wendet ihre standardmäßige Kundenidentifizierungsprozedur an (Signaturkarten, Mitarbeiteraufzeichnungen, persönliche Informationen usw.), bevor das Individuum im System registriert wird. Es ist wichtig, dass die Institution die Identität des Individuums so sorgfältig wie möglich verifiziert, da das registrierende Individuum ermächtigt ist, Geld von diesen Konten nach seinem Gutdünken zu übertragen und/oder elektronische Nachrichten unter dem Namen des Unternehmen zu versenden.

1.4.8.4. Funktionsweise

[0344] Während der Registrierung gibt das Individuum sowohl primäre als auch sekundäre biometrische Daten ein. Das Individuum muss beide Zeigefinger verwenden; wenn dieser Person die Zeigefinger fehlen, kann der nächste innen liegende Finger verwendet werden. Die Anforderung, spezifische Finger zu verwenden, ermöglicht das Funktionieren der Vorab-Betrugskontrolle.

[0345] Das Individuum wird gebeten, einen Haupt- und einen Nebenfinger auszuwählen. Der Hauptfinger wird während der DPC-Identitätskontrolle bevorzugt behandelt, so dass das Individuum den zumeist verwendeten Finger als Hauptfinger angeben sollte. Natürlich könnte das DPC beschließen, die Kennzeichnung primärer und sekundärer biometrischer Daten zu verändern, wenn sich dies als wichtig herausstellen sollte.

[0346] Als Teil des biometrischen Codiervorgangs bestimmt die BIA/Reg, ob das Individuum einen „guten Abdruck" hinterlassen hat. Es ist zu beachten, dass es einige Individuen gibt, die im Laufe ihrer Arbeit zufällig ihren Fingerabdruck einbüßen, z. B. Menschen, die Schleifmitteln oder Säuren hantieren. Leider können diese Personen das System nicht verwenden. Sie werden in dieser Phase des Vorgangs detektiert und informiert, dass sie nicht teilnehmen können.

[0347] Das Individuum wählt einen PIC aus vier bis zwölf Stellen einer Reihe von PIC-Optionen aus, die die zentrale Datenbank des Systems liefert. Dies umfasst zwei Kontrollen: Erstens darf die Zahl anderer Individuen, die den gleichen PIC verwenden, nicht zu hoch sein (da der PIC dazu dient, die Anzahl an Individuen zu reduzieren, die durch den biometrischen Vergleichsalgorithmus überprüft werden), und zweitens darf das die Registrierung durchlaufende Individuum biometrisch gesprochen nicht zu viele Ähnlichkeiten mit anderen Individuen innerhalb derselben PIC-Gruppe aufweisen. Wenn dies eintritt, wird die Anmeldung abgewiesen, eine Fehlermeldung wird an das BRT zurückgeschickt, und das Individuum wird angewiesen, einen anderen PIC anzufordern. Das System kann gegebenenfalls die Fehlermeldung „identische Übereinstimmung" zurückschicken – dies bedeutet, dass das Individuum bereits einen Eintrag im System unter diesem PIC hat.

[0348] Ein PIC von 0 ermöglicht dem System, dem Individuum einen PIC zuzuteilen.

[0349] Das Individuum konstruiert einen vertraulichen Code, der aus einem Wort oder einer Phrase besteht. Wenn das Individuum keinen derartigen privaten Code erstellen möchte, wird er wahllos vom Endgerät konstruiert.

[0350] Das Individuum kann auch seine Finanzkontencodeliste ordnen. Diese Liste beschreibt, welcher Kontoindexcode für welches Konto steht (d. h. 1 für Lastschrift, 2 für Gutschrift, 3 für Notfalls-Lastschrift usw.). Es ist zu beachten, dass dies nur eintreten kann, wenn die registrierende Stelle eine Bank ist und wenn die Konten im Besitz dieser Bank stehen.

[0351] Sogar nach der Registrierung kann das Individuum erst dann Vorgänge unter Zuhilfenahme des Systems durchführen, wenn eine Vorab-Betrugskontrolle abgeschlossen ist. Dies dauert im Allgemeinen einige Minuten, doch während Zeiten hoher Belastung kann dieser Vorgang mehrere Stunden in Anspruch nehmen. Nur wenn das System keinen vorherigen Betrug festgestellt hat, wird das Konto des Individuums aktiviert.

1.4.8.5. Sicherheit

[0352] Wenn ein Individuum das System auch nur einmal missbraucht hat, beginnt das DPC mit einer Datenbank-weiten unfreiwilligen biometrischen Suche nach dem Täter. Mehrere davon werden jede Nacht durchgeführt, so dass Individuen, nach denen das System besonders intensiv sucht, unter Anwendung eines zeitaufwendigen Verfahrens während Phasen geringer Aktivität ausgesiebt werden.

[0353] Die den Registrierungsvorgang durchführenden Mitarbeiter identifizieren sich mittels Biometrik-PIC nur dann, wenn zunächst das Registrierungssystem aktiviert wurde. Dies ist für den betreffenden Mitarbeiter praktisch, stellt aber ein mögliches Sicherheitsproblem für das System dar, da unbeaufsichtigte oder „vorübergehend verborgte" BRTs dem Betrug Vorschub leisten könnten. In der Folge wird die Registrierungsanmeldung nach Ablauf einer vorbestimmten Zeitspanne ohne Aktivität gestoppt.

1.4.9. Endgerät: Kundendienst

1.4.9.1. Zweck

[0354] Der Zeck des Kundendienst-Endgeräts (CST) besteht darin, internen DPC-Support-Personalzugriff auf verschiedene Teile der Systemdatenbanken zu ermöglichen. Die Support-Mitarbeiter müssen Fragen von Individuen, Ausgebestellen, Institutionen und Händlern beantworten, die Schwierigkeiten mit dem System haben.

1.4.9.2. Konstruktion

[0355] Das CST besteht aus Folgendem:
- ein Mikrocomputer
- eine BIA/Int
- eine Ethernet/Token Ring/FDDI Netzwerk-Schnittstelle
- eine Datenbankkontrolle und Modifikationsapplikation

[0356] Jedes CST ist über eine Hochgeschwindigkeits-LAN-Verbindung wie z. B. Token Ring, Ethernet, Faser (FDDI) usw. mit dem System verbunden. Jedes CST hat die Fähigkeit, jede der Datenbanken abzufragen und die Ergebnisse dieser Abfragen anzuzeigen. Doch das CST zeigt Felder und Einträge nur je nach den Privilegien des individuellen Endgerätebenutzers an. Ein durchschnittlicher Kundendienstmitarbeiter z. B. ist nicht in der Lage, den Verschlüsselungscode für einen VDB-Eintrag einer bestimmten BIA zu erfahren, obwohl er feststellen kann, welcher Händler oder welches Individuum derzeit diese BIA besitzt.

1.4.9.3. Identifizierung

[0357] Damit das CST Zugriff auf die Datenbank erlaubt, müssen das Individuum und die BIA vom System identifiziert werden. Außerdem muss der Privilegiertenstatus des Individuums ermittelt werden, so dass die Datenbank den Zugriff entsprechend einschränken kann.

1.4.9.4. Funktionsweise

[0358] Ein Individuum, das ein CST verwendet, beginnt eine Sitzung, indem es sich durch Eingabe seines Biometrik-PIC identifiziert. Die BIA konstruiert eine Identifizierungs-Aufforderungsnachricht und schickt sie dann zur Verifizierung an das DPC. Sobald das System das Individuum verifiziert hat, kann die CST-Anwendung normal funktionieren, obwohl sie durch die zuvor dem Individuum zugeteilte DCP-Privilegstufe beschränkt ist.

1.4.9.5. Sicherheit

[0359] Aus Sicherheitsgründen beendet das DPC nach einer vorbestimmten Leerlaufzeit die Verbindung zur CST-Anwendung.

[0360] Es ist wichtig, dass die Datenbankapplikation in keiner Weise – entweder absichtlich oder durch unbeabsichtigtes Einschleusen eines Virus – modifiziert wird. Zu diesem Zweck besitzen einzelne CST keine Diskettenlaufwerke oder andere entfernbare Medien. Außerdem ist der Lesezugriff auf das Ausführungsprogramm der Datenbankapplikation strikt auf jene beschränkt, die etwas wissen müssen.

[0361] Um die Kommunikation zwischen dem CST und der Datenbank vor heimlicher Modifikation oder Offenlegung zu schützen, verschlüsselt das CST den gesamten Verkehr zwischen dem CST und der Datenbank. Dazu erzeugt das CST einen Session Key, der während der Anmeldesitzung im System dem Server zugeschickt wird. Dieser Session Key dient zum Verschlüsseln und Entschlüsseln aller Kommunikationen mit dem DPC, die während dieser Zeit anfallen.

[0362] Selbst unter der Annahme, dass die Kommunikationen sicher ablaufen und keine Datenbankapplikationen modifiziert werden, stellt das DPC sicher, dass DPC-Datenfelder, die für das das CST bedienende Individuum nicht zugreifbar sind, nicht der Datenbankapplikation des CST übermittelt werden. Ebenso haben CST-Mitarbeiter zu keinem Zeitpunkt Zugriff auf die Modifikation individueller biometrischer Informationen bzw. die Erlaubnis, diese Modifikationen durchzuführen.

[0363] Das DPC und das Supportcenter können an einem Ort untergebracht oder aufgrund der strengen Sicherheitsvorschriften betreffend das CST selbst voneinander getrent sein.

1.4.10. Endgerät: Ausstellerendgerät

1.4.10.1. Zweck

[0364] Der Zweck des Ausstellerendgeräts besteht darin, Mitarbeiter in ausstellenden Banken in die Lage zu versetzen, Finanzkonto-Batch-Modifikationsvorgänge dem DPC sicher und identifizierbar vorzulegen.

1.4.10.2. Konstruktion

[0365] Das IT besteht aus Folgendem:
- ein Mikrocomputer
- ein Modem-, X.25-Netwerk- oder Internetverbindung zum System
- ein BIA/Iss
- eine Netzwerkverbindung zum internen Banknetz

[0366] Das IT benutzt eine Aussteller-BIA, um Massenhinzufügungen und -löschungen von Finanzkontoinformationen zu autorisieren.

1.4.10.3. Identifizierung

[0367] Bei diesem Vorgang muss die Bank identifiziert werden, ein entsprechend autorisierter Bankangestellter muss ebenfalls identifiziert werden, und alle Individuen, deren Finanzkonten hinzugefügt oder entfernt werden, müssen auch identifiziert werden.

[0368] Die Bank ist für die Identifizierung von Individuen zuständig, die ihre Konten bei dieser Bank ihrer Finanzkontoliste hinzufügen wollen. Wie im Fall der biometrischen Registrierung erfolgt dies, indem die Bank Signaturkarten und persönliche Informationen verwendet. Das DPC identifiziert die Bank durch Gegenvergleich des vom IT vorgelegten Ausstellercodes mit dem im VAD-Eintrag von BIA/Iss registrierten Ausstellercode. Ein Biometrik-PIC identifiziert den Bankangestellten, der den Batch tatsächlich vorlegt.

1.4.10.4. Funktionsweise

[0369] Damit ein Finanzkonto hinzugefügt werden kann, gibt ein Individuum der Bank seine biometrische Identifizierungsnummer (die Identifizierungsnummer wird dem Individuum während des anfänglichen biometrischen Registrierungsschritts mitgeteilt) sowie die hinzuzufügenden Konten bekannt. Nach der ordnungsgemäßen Identifizierung des Individuums werden dieser Identifizierungscode und die Kontoliste zwecks nachfolgender Batchvorlage im System an das IT weitergeleitet.

[0370] Eine autorisierte Person in der Bank weist das IT an, die gestapelten Hinzufügungen bzw. Löschungen in das DPC hochzuladen, wenn die Bank dies als angemessen erachtet. Dazu gibt die autorisierte Person ihren Biometrik-PIC ein, das IT fügt einen Session Key und den Ausstellercode der Bank hinzu, und BIA/Iss konstruiert daraufhin eine Ausstellerbatch-Aufforderungsnachricht, die das IT dann an das DPC weiterleitet. Das IT verschlüsselt den Batch unter Verwendung des Nachrichtencodes und schickt dann auch diesen ab.

[0371] Wenn das System die Ausstellerbatch-Aufforderung erhält, validiert sie, dass die BIA eine BIA/Iss ist,

dass die BIA/Iss bei der vom Ausstellercode bezeichneten Bank registriert ist und dass das im Biometrik-PIC identifizierte Individuum Batch-Aufforderungen dem DPC für diese Bank vorlegen kann. Wenn dies der Fall ist, verarbeitet das DPC alle diese Anfragen und vermerkt auch allenfalls auftretende Fehler. Sobald dies geschehen ist, sendet das DPC den privaten Code des Individuums sowie einen verschlüsselten Batch zurück, der allenfalls während der Verarbeitung aufgetretene Fehler enthält.

1.4.10.5. Sicherheit

[0372] Das Sichern dieser Transaktion ist für die Sicherheit des Systems entscheidend. Ein Krimineller braucht in betrügerischer Absicht lediglich eine Möglichkeit ausfindig machen, wie er die Konten anderer Menschen seinem biometrischen Identifizierungscode hinzufügen kann – dann ist er in der Lage, nach Belieben betrügerische Handlungen vorzunehmen. Schlussendlich wird der Kriminelle wohl gefasst und aus der Datenbank gelöscht, aber erst nachdem die Konten anderer Personen von diesem Kriminellen geleert wurden.

[0373] Die Verschlüsselung garantiert, dass die Übertragung zwischen Bank und DPC nicht aufgefangen werden kann, wodurch Kontonummern während dieser Übermittlung geschützt sind.

[0374] Der Gegenvergleich der Bank mit der BIA/Iss sorgt dafür, dass sowohl das IT als auch die BIA in ihrer Funktionsweise beeinträchtigt sein müssten, um fehlerhafte Hinzufügungs- bzw. Löschungsnachrichten an das DPC zu senden. Somit muss die Bank gewährleisten, dass das IT physikalisch sicher ist und dass nur autorisierte Individuen Zugriff darauf haben.

[0375] Die Anforderung, dass ein Individuum den Stapel vorlegt, bedeutet, dass diese Person verantwortungsbewusst handelt und weiß, was „auf dem Spiel steht"; ihre Aufgabe besteht darin, sicherzustellen, dass die richtigen Banksicherheitsmaßnahmen bei der Konstruktion und Vorlage des Stapels ergriffen wurden.

1.4.11. Endgerät: Geldausgabeautomat (ATM)

1.4.11.1. Zweck

[0376] Der Zweck von Biometrik-ATM besteht darin, Individuen Zugang zu Bargeld und anderen Geldausgabeautomat-(ATM-) Funktionen zu gewähren, ohne dazu eine Interbankkarte verwenden zu müssen. Dies geschieht, indem ein Biometrik-PIC und ein Kontoindexcode vorgelegt und eine Bankkontonummer abgerufen werden. Für Benutzer des Systems ist dadurch der Mechanismus Interbankkarte (auf dem Gebiet der Erfindung bekannt) + PIC als Verfahren zur Identifizierung des Kontos und Autorisierung des Individuums überflüssig. Man nimmt an, dass alle Geldausgabeautomaten weiterhin Interbankkarten akzeptieren.

1.4.11.2. Konstruktion

[0377] Ein ATM-Endgerät besteht aus Folgendem:
- ein Standard-Geldausgabeautomat
- eine integrierte BIA/ATM (nur Scanner)
- eine Verbindung zum DPC

[0378] Der Biometrik-ATM arbeitet mit integrierter BIA/ATM, um Individuen zu identifizieren und ihnen den Zugang zu Finanzkonten unter Verwendung eines Biometrik-PIC und eines Kontoindex zu gewähren. BIA/ATM ist im Geldausgabeautomat installiert, wobei das jeweilige PIC-Feld des Geldausgabeautomaten für die Eingabe von PIC und Kontoindexcode verwendet wird. Der Geldausgabeautomat (ATM) ist mit dem System über X.25 oder Modem verbunden.

[0379] Die BIA/ATM ist solcherart aufgebaut, dass die Integration mit einem bestehenden ATM-Netzwerk so einfach wie möglich ist. Dadurch muss ein Kompromiss zwischen Sicherheit und Integrationsfreundlichkeit eingegangen werden.

1.4.11.3. Identifizierung

[0380] Es müssen drei Teilnehmer identifiziert sein, damit das DPC richtig auf eine BIA/ATM-Kontoabfrage reagieren kann: das Individuum, die Bank und BIA/ATM.

[0381] Die Bank wird durch Vergleichen des gespeicherten Bankcodes des Geldausgabeautomaten mit dem

BIA/ATM-Bankcode identifiziert. Die BIA/ATM wird dann durch erfolgreiches Lokalisieren von BIA/ATM in der VAD und das Individuum durch Standard-Biometrik-PIC identifiziert.

1.4.11.4. Funktionsweise

[0382] Um auf einen Geldausgabeautomaten zugreifen zu können, gibt ein Individuum seinen Biometrik-PIC sowie den Kontoindexcode in die BIA ein. Die BIA erstellt eine Kontozugriffs-Aufforderungsnachricht, die dann durch den Geldausgabeautomaten an das DPC geschickt wird. Das DPC validiert den Biometrik-PC sowie den Notfall-Kontoindexcode und sendet die resultierende Finanzkontonummer sowie den privaten Code an den Geldausgabeautomaten zurück.

[0383] Der Geldausgabeautomat bittet die BIA, die Antwort zu entschlüsseln, und zeigt den privaten Code auf dem Anzeigeschirm des Geldausgabeautomaten an. Dieser untersucht auch die Antwort, um festzustellen, ob das Individuum einen standardmäßigen Kontozugriff oder einen Kontozugriff „in Not" vornimmt. Wenn ein Kontozugriff in Not gemeldet wird, kann der Geldausgabeautomat falsche oder irreführende Informationen über die für das Individuum verfügbaren Geldbeträge geben; die genaue Verhaltensweise ist hier von Geldausgabeautomat zu Geldausgabeautomat unterschiedlich. Kein Geldausgabeautomat teilt aber dem Individuum jemals mit, dass derzeit ein Vorgang in Not abgewickelt wird.

1.4.11.5. Sicherheit

[0384] Nachrichten zwischen dem Geldausgabeautomaten (ATM) und dem DPC sind durch Verschlüsselung und MAC-Berechnung anhand der BIA gesichert. Der MAC bedeutet, dass der Geldausgabeautomat den Inhalt der Nachricht nicht verändern kann, ohne detektiert zu werden, und die Verschlüsselung verhindert die Offenlegung des verschlüsselten Teils der Nachricht.

[0385] Da die BIA/ATM keinen angefügten LCD-Schirm oder kein angefügtes PIC-Feld besitzt, ist es nötig, dass der Geldausgabeautomat alle Textaufforderungen liefert und alle Eingaben des Individuums erfasst. Dies ist weniger sicher, als wenn die BIA den Vorgang durchführen würde, doch da Geldausgabeautomaten üblicherweise physikalisch robust sind, halten sich die Dinge hier in der Waage.

1.4.11.6. Anmerkungen

[0386] Zwischen der Bank und dem Individuum ist die Verhaltensweise eines Geldausgabeautomaten festzulegen, wenn das Individuum angibt, dass es eine Transaktion in Not durchführt. Es gibt Banken, die den Zugriff einschränken oder Konto- bzw. Saldoinformationen verändern, oder es kann auch ein falscher Schirm angezeigt werden. Ein falscher Schirm ist eine Datenanzeige, die absichtlich unpräzise ist, so dass eine Zwang ausübende Person nicht unbefugt Zugriff auf präzise Daten zu den Finanzkonten eines Individuums erhält. Es liegt außerhalb des Schutzbereichs der Erfindung, die genaue Verhaltensweise eines Geldausgabeautomaten unter diesen Umständen festzulegen.

1.4.12. Endgerät: Telefon-Kassenendgerät (PPT)

1.4.12.1. Zweck

[0387] Der Zweck des PPT besteht darin, Gut- oder Lastschrift-Finanztransaktionen von einem Individuum zu autorisieren, das mittels eines speziell ausgerüsteten Telefons einen Einkauf bei einem Händler tätigt.

1.4.12.2. Konstruktion

[0388] Das PPT besteht aus Folgendem:
- eine BIA/catv
- ein digitales Schnellverbindungsmodem [siehe VoiceView-Patent (auf dem Gebiet der Erfindung bekannt)]
- ein Telefon (Tastenfeld, Hörer, Mikrofon)
- ein Mikroprozessor
- ein DSP (digitaler Signalprozessor)
- eine Standardtelefonleitung

[0389] Das PPT akzeptiert die biometrische Identifizierung unter Verwendung einer BIA/catv, die mit einem

Schnurlos-, Mobil- oder Standardtelefon verbunden und damit integriert ist.

1.4.12.3. Identifizierung

[0390] Damit das DPC eine Transaktion autorisiert, müssen sowohl das Individuum als auch der Händler identifiziert sein.

[0391] Um ein Individuum zu identifizieren, muss auf Biometrik-PIC-Identifizierung zurückgegriffen werden.

[0392] Um einen Händler, der Telefonbestellungen anbietet, zu identifizieren, werden der Händler und alle seine Telefonnummern, die Individuen anrufen, beim DPC gespeichert. Wenn somit ein Individuum eine Autorisierung vorlegt, legt es auch die von ihm angerufene Telefonnummer vor, die dann mit den eingetragenen Telefonnummern des Händlers verglichen und überprüft werden.

1.4.12.4. Funktionsweise

[0393] Individuen rufen Händler an, die ihre Waren über Kataloge in Papierform, Zeitungen, Zeitschriften oder andere Printmedien anbieten. Das PPT arbeitet mit einem speziellen Modem, das sich der Telefonsprachleitung bedient, um digitale Informationen mit dem Händler auszutauschen.

[0394] Jedes Mal, wenn der Benutzer einen Anruf tätigt, verzeichnet das PPT die eingegebene Telefonnummer, sollte er sich entscheiden, einen Kauf zu tätigen. Ein DSP dient zum Detektieren des Ruftons, des Läutens, der Verbindung usw., um mitzuteilen, welche tatsächliche Telefonnummer (im Gegensatz zu Nebenstellennummern) eingegeben wurde, oder zur Navigation von Telefonnachrichtensystemen usw.

[0395] Sobald ein Anruf bei einem Händler einlangt, lädt ein Verkäufer im Händlerlokal alle relevanten Informationen in das PPT herunter (z. B. Produkt, Preis, Händlercode). Es ist zu beachten, dass das Modem im Betrieb die Sprecherverbindung unterbricht.

[0396] Wenn die Produktinformationen heruntergeladen sind, fordert das PPT das Individuum auf, den Biometrik-PIC und den Kontoindexcode einzugeben, und bittet das Individuum dann, den Kaufbetrag zu validieren. Dann werden die Telefonnummer und der Händlercode hinzugefügt und die Nachricht verschlüsselt. Das Schnellverbindungsmodem wird wieder dazu benutzt, die Autorisierungsinformation dem Händler zukommen zu lassen.

[0397] Wenn der Händler die Autorisierungsinformation erhält, verifiziert er, dass die Preis- und Produktinformationen korrekt sind und leitet dann die Transaktion an das DPC weiter; dabei bedient er sich eines gesicherten Kommunikationskanals über das Internet oder ein anderes nicht spezialisiertes Netzwerk. Die Verbindung mit dem DPC wird durch Public Key-Verschlüsselung und Austausch von Geheimschlüsseln gesichert.

[0398] Nach Erhalt und Entschlüsselung einer Telefonautorisierung überprüft das DPC die Telefonnummer und vergleicht sie mit dem Händlercode, validiert den Biometrik-PIC und sendet danach zwecks Autorisierung die Transaktion an das Lastschrift/Gutschrift-Netzwerk. Wenn die Autorisierung erfolgreich ist, fügt das DPC die Adresse des Käufers n die Antwortnachricht an, und schickt dem Händler eine Antwort.

[0399] Der Händler erhält die Antwort vom DPC, kopiert die Zustelladresse und leitet die Nachricht wiederum über eine kurze Sitzungsverbindung mit dem Schnellverbindungsmodem an das Individuum weiter. Wenn die Übertragung an das IPT abgeschlossen ist, ertönt ein Signal, das Modem trennt die Verbindung, und der private Code des Individuums (durch die BIA verschlüsselt) wird auf dem LCD-Schirm angezeigt. Der Verkäufer des Händlers bestätigt, dass die Zustelladresse des Individuums gültig ist; wenn dies der Fall ist, wird der Anruf beendet, und die Transaktion ist abgeschlossen.

1.4.12.5. Sicherheit

[0400] Einer der Sicherheitsaspekte bei Telefontransaktionen ist die Sicherheit des Telefonsystems selbst. Neben der biometrischen Identifizierung liegt das Hauptproblem darin, sicherzustellen, dass die vom Individuum angerufene Telefonnummer tatsächlich zum betroffenen Händler führt.

[0401] Es ist zu beachten, dass die Kommunikationsverbindung zwischen dem PPT und dem Händler nicht gesichert ist, weshalb eine Kaufautorisierung von einem Individuum zu einem Händler abgefangen werden

könnte. Es lässt sich daraus jedoch kein finanzieller Nutzen ziehen, so dass dieser Aspekt nicht als wesentlich eingestuft wird.

[0402] Die Sicherheit eines PPT ist aufgrund des Preises und Gewichts sowie aufgrund der Problematik, die Verantwortung zwischen PIC-Eingabe und Entschlüsselung und Präsentation des privaten Codes aufzuteilen, verhältnismäßig gering.

1.4.13. Endgerät: Kabel-TV-Kasse

1.4.13.1. Zweck

[0403] Der Zweck der CATV-Kasse (CATV-CPT) liegt darin, Last- oder Gutschrifts-Finanztransaktionen von einem vor seinem Fernsehgerät sitzenden Individuum zu einem Händler, der seine Waren im Fernsehen zum Verkauf anbietet, zu autorisieren.

1.4.13.2. Konstruktion

[0404] Das CPT besteht aus Folgendem:
- eine BIA/catv
- eine TV-Fernbedienung mit integrierter BIA/catv
- ein Kabel-TV-Digitalsignaldecoder
- ein Kabel-TV-Fernbedienungslesegerät
- ein Schirmanzeigemechanismus
- ein Zugang zu einem bidirektionalen Kabel-TV-Breitband-Kommunikationskanal

[0405] Das CPT akzeptiert biometrische Identifizierung mittels BIA/catv (mit der TV-Fernbedienung integriert). Die Fernbedienung kommuniziert mit einer TV-Top-Box, die ihrerseits mit dem Breitbandfernsehnetz kommuniziert. Das Endgerät besteht aus der TV-Fernlogik, die mit der BIA kommuniziert, sowie aus der TV-Top-Box, die über das Kabelbreitbandnetz kommuniziert.

1.4.13.3. Identifizierung

[0406] Bei dieser Transaktion müssen sowohl der Händler als auch das Individuum identifiziert sein, um die Transaktion durchzuführen.

[0407] Das Individuum ist durch den Biometrik-PIC identifiziert.

[0408] Der Händler ist durch ein Händler-Akkreditiv, das von der CATV-Sendestation generiert wird, wenn das Produkt im Fernsehen präsentiert wird, identifiziert. Jede Produktpräsentation im Fernsehen ist mit einem Händler-Produkt-Akkreditiv versehen, das aus einem Händlercode, einem Zeitpunkt, einer Zeitdauer und einem Preis besteht, der mittels Public Key-Verschlüsselung und dem privaten Schlüssel der CATV-Netz-Sendestation signiert ist. Dieses Händler-Produkt-Akkreditiv kann nur von der Fernsehnetzsendeanstalt generiert werden.

1.4.13.4. Funktionsweise

[0409] Wenn in der Fernsehwerbung, in Infomercials oder auf einem Home Shopping-Fernsehkanal Produkte präsentiert werden, strahlt das Kabel-TV-Netz auch gleichzeitige digitale Informationen aus (Kurzbeschreibung, Preis, Händler-Produkt-Akkreditiv). Diese digitalen Informationen werden verarbeitet und vorübergehend im CPT gespeichert und können vom Individuum abgerufen werden, wenn die Kaufentscheidung getroffen wurde.

[0410] Um ein gerade angezeigtes Produkt kaufen zu können, wählt das Individuum die Schirmanzeigefunktion der Spezialfernbedienung, die das CPT anweist, Textinformationen über das derzeit präsentierte Produkt auf dem Schirm anzuzeigen.

[0411] Der Benutzer wird zuerst über die Schirmanzeige nach der Nummer der Produkte gefragt, die er kaufen möchte. Dann wird er gebeten, seinen Biometrik-PIC und seinen Kontoindexcode einzugeben. Sobald er verifiziert hat, dass der endgültige Kaufpreis in Ordnung geht, werden der Produktpreis, der Händlercode, das Händler-Produkt-Credential und die Kanalnummer sowie der Biometrik-PIC dazu herangezogen, einer

Fern-Transaktionsautorisierungs-Aufforderungsnachricht zu erstellen. Die Aufforderung wird über den bidirektionalen Kabel-TV-Breitband-Kommunikationskanal zwecks Autorisierung an den Händler geschickt.

[0412] Es ist zu beachten, dass jeder Händler, der Produkte auf diese Weise verkaufen möchte, die Fähigkeit besitzen muss, Bestellungsinformationen unter Verwendung des Breitband-Kabel-TV-Netzes zu empfangen.

[0413] Nach Erhalt der Autorisierungsaufforderung legt der Händler diese über eine gesicherte Internet- oder X.25-Verbindung dem DPC vor.

[0414] Wenn das DPC die Transaktion autorisiert, erstellt es eine Autorisierungsantwort, die die aktuelle Zustelladresse des Individuums sowie den Autorisierungscode und den verschlüsselten privaten Code enthält. Sobald der Händler die Autorisierung erhält, kopiert er die Autorisierung und die Zustelladresse und leitet die Autorisierung dann zurück an das CPT, das dann dem Individuum den privaten Code anzeigt, wodurch der Vorgang abgeschlossen ist.

1.4.13.5. Sicherheit

[0415] Diese Architektur erlaubt es Kriminellen nicht, vom Kabel-TV-Breitband abgefangene Nachrichten wiederzugeben, doch sie sind in der Lage, Teile davon zu lesen. Wenn dies nicht erwünscht ist, können die Nachrichten mittels eines optionalen CATV Center-Public Key oder mittels einer anderen „Link-Level"-(Verbindungsebenen-) Verschlüsselung zwischen der CATV-Set-Top-Box (auf dem Gebiet der Erfindung bekannt) und dem lokalen CATV-Büro verschlüsselt werden.

[0416] Um eine Verbindung zwischen einem Händler und dem DPC zu sichern, verwendet die Verbindung einen täglich wechselnden Session Key, der zuvor mittels eines Public Key-Verschlüsselungs-Schlüsselaustauschsystems ausgetauscht wurde.

1.5. Systembeschreibung: Datenverarbeitungszentrum

1.5.1. Einführung

[0417] Das DPC wickelt vor allem Finanztransaktions-Autorisierungen und individuelle Registrierungen ab. Darüber hinaus ist das DPC für das Speichern und Abrufen gesicherter Faxnachrichten, elektronischer Dokumente und elektronischer Signaturen verantwortlich.

[0418] Jeder DPC-Standort besteht aus einigen Computern und Datenbanken, die über ein LAN (auf dem Gebiet der Erfindung allgemein bekannt) miteinander verbunden sind, wie dies in der DPC-Übersicht (Fig. **) dargestellt ist. Mehrere identische DPC-Standorte stellen zuverlässigen Service im Katastrophenfall oder bei gravierendem Hardwareversagen an einem beliebigen DPC-Standort sicher. Außerdem verfügt jeder DPC-Standort in allen kritischen Hard- und Softwaresystemen über Notstromaggregate und multiple Redundanzen.

[0419] Die DPC-Komponenten fallen in drei Kategorien: Hardware, Software und Datenbanken. Es folgt eine kurze Beschreibung jeder Komponente nach Kategorien. Ausführliche Beschreibungen finden sich in den anschließenden Abschnitten.

1.5.1.1. Hardware

FW Firewall-Vorrichtung: der Eingangspunkt des DPS-Standorts
GM Gateway-Vorrichtung: der Systemkoordinator und Nachrichtenprozessor
DPCLAN DPC Local Area Network: verbindet die DPC-Standorte miteinander

1.5.1.2. Datenbanken

IBD Individuelle biometrische Datenbank (Individual Biometric Database): identifiziert Individuen anhand ihres Biometrik- und PIC-Codes.
PFD Datenbank über vorherigen Betrug (Prior Fraud Database): listet jene Individuen aus, die das System missbraucht haben, und überprüft, ob eine biometrische Eingabe mit diesen Individuen übereinstimmt.
VAD Datenbank betreffend die Validität der Vorrichtung (Valid Apparatus Database): speichert Informationen zum Validieren und Entschlüsseln von BIA-Nachrichten.
AOD Datenbank betreffend die Besitzer der Vorrichtungen (Apparatus Owner Database): speichert Informati-

onen über die Besitzer von BIA-Vorrichtungen.
ID Ausstellerdatenbank (Issuer Database): ausstellende Banken, die am System teilnehmen.
AID Datenbank über autorisierte Individuen (Authorized Individual Database): speichert die Liste von Individuen, die persönlice oder Aussteller-BIA-Vorrichtungen verwenden dürfen.
RMD Datenbank für den Händler-Fernverkauf (Remote Merchant Database): speichert Informationen zur Verarbeitung von Transaktionen mit Telefon- und Kabel-TV-Händlern.
EDD Datenbank für elektronische Dokumente (Electronic Document Database): speichert elektronische Dokumente wie z. B. Faxnachrichten und E-Mails, um von autorisierten Individuen aufgerufen zu werden.
ESD Datenbank für elektronische Signaturen (Electronic Signature Database): speichert elektronische Dokumentsignaturen zwecks Verifizierung durch einen Dritten.

1.5.1.3. Software

MPM Nachrichten-Verarbeitungsmodul (Message Processing Module): ist für die Verarbeitung jeder Nachricht durch Koordination mit den anderen Softwaremodulen und Datenbanken verantwortlich, die zur Erfüllung der im Zusammenhang mit der Nachricht anfallenden Aufgaben notwendig sind.
SNM Folgenummermodul (Sequence Number Module): übernimmt die DUKPT-Folgenummerverarbeitung.
MACM Nachrichtenauthentifizierungs-Codemodul (Message Authentication Code Module): ist für die MAC-Validierung und -Generierung zuständig.
MDM Nachrichtentschlüsselungsmodul (Message Decrypt Module): ist für die Verschlüsselung und Entschlüsselung von BIA-Aufforderungen und -Antworten verantwortlich.
PGL PIC-Gruppen-Liste (PIC Group List): übernimmt die Durchsicht der PIC-Gruppen nach PIC und die Konfiguration von Datenbankelementen, die von der Liste von PIC-Gruppen abhängen.
IML IBD-Maschinen-Liste (IBD Machine List): ist für die Durchsicht der Haupt- und Sicherungsdatenbankmaschinen zuständig, in denen IBD-Aufzeichnungen für eine bestimmte PIC-Gruppe gespeichert sind.

1.5.1.4. Terminologie

[0420] Bei der Definition des Datenbankschemas wird zur Beschreibung von Feldtypen die folgende Terminologie verwendet:

int<X>	integrierter Typ mit <X> Bytes Speicher
char<X>	Zeichenbereich von <X> Bytes
text	Zeichenbereich variabler Länge
<type>[X]	Länge <X>-Bereich des spezifizierten Typs
time	Typ zum Speichern von Zeit und Datum
biometric	Binärer Datentyp zum Speichern der Biometrie
fax	Binärer Datentyp zum Speichern von Faxbildern

[0421] Bei der Beschreibung von Datenbankspeicheranforderungen bezieht sich der Ausdruck „erwartet" auf den erwarteten Zustand eines voll geladenen Systems.

1.5.2. Protokollbeschreibung

[0422] Endgeräte bewältigen ihre Aufgaben, indem sie Anfragepakete an einen DPS-Standort schicken. Dieser schickt ein Antwortpaket zurück, das den Status der Aufforderung (erfolgreich oder fehlgeschlagen) enthält.

[0423] Die Kommunikation erfolgt über einen logischen oder einen physikalischen verbindungsorientierten Nachrichtenzustellmechanismus wie z. B. X.25-Verbindungen, TCP/IP-Verbindungen oder einen Telefonanruf an eine Modembank. Jede Sitzung hält die Verbindung zum Endgerät offen, bis das DPC seine Antwort zurück an das Endgerät schickt.

[0424] Das Anfragepaket enthält einen BIA-Nachrichtenteil und einen Endgerätnachrichtenteil.

BIA-Nachrichtenteil

Protokollversionsnummer

Nachrichtentyp

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

<nachrichtenspezifische Daten>

Nachrichten-Authentifizierungscode (MAC)

Endgerätnachrichtenteil

<endgerätspezifische Daten>

[0425] Der BIA-Nachrichtenteil wird von einer BIA konstruiert. Er enthält eine oder zwei biometrische Angaben, einen PIC, Autorisierungsbeträge und den Inhalt der allgemeinen Register (vom Endgerät bestimmt). Es ist zu beachten, dass der MAC im BIA-Nachrichtenteil nur auf den BIA-Teil und nicht auf den Endgerätteil zutrifft.

[0426] Ein Endgerät kann in jedem Endgerätnachrichtenteil zusätzliche Daten für die Aufforderungsnachricht unterbringen. Die BIA bietet einen Nachrichtenschlüssel, damit das Endgerät die Daten des Endgerätteils sichern kann. Falls dies erforderlich ist, inkludiert die BIA automatisch den Nachrichtenschlüssel im verschlüsselten Biometrik-PIC-Block des Pakets. Das Endgerät führt jedoch die Nachrichtenschlüssel-Verschlüsselung selbst durch.

[0427] Das Antwortpaket enthält einen Standardkopfteil und zwei optionale Nachrichtenteile beliebiger Form: einen mit einem MAC und einen ohne:

Standardkopfteil

Protokollversionsnummer

Nachrichtentyp

Optionaler Nachrichtenteil beliebiger Form mit MAC

<nachrichtenspezifische Daten>

MAC

Optionaler Nachrichtenteil beliebiger Form ohne MAC

<zusätzliche nachrichtenspezifische Daten>

[0428] Der Nachrichtenteil mit einem MAC wird an die BIA geschickt, so dass sie bestätigen kann, dass dieser Teil der Antwort nicht manipuliert wurde, und der private Code des Individuums angezeigt werden kann. Der Nachrichtenteil ohne MAC dient zur Übermittelung großer Datenmengen wie z. B. von Faxbildern, die nicht der BIA zwecks MAC-Validierung zukommen, da die BIA-Endgerät-Verbindung nur beschränkte Bandbreite aufweisen kann.

1.5.3. Verarbeitungspakete

[0429] In einer Ausführungsform der Erfindung mit mehreren DPC-Standorten muss ein Endgerät lediglich seine Anfrage an einen der DPC-Standorte schicken (üblicherweise den nächstgelegenen), da dieser automatisch die anderen updatet, indem – falls dies erforderlich ist – dezentrale (distributed) Transaktionen gestartet werden.

[0430] Wenn eine der Firewall-Vorrichtungen des DPC ein Paket empfängt, wird es zur eigentlichen Verarbei-

tung an eine der GM-Vorrichtungen weitergeleitet. Jede GM besitzt ein MPM (Message Processing Module), das für die Koordination zwischen den für die Abwicklung der Anfrage notwendigen DPC-Komponenten zuständig ist, und schickt die Antwort an den Absender zurück.

1.5.4. Validierungs- und Entschlüsselungspakete

[0431] Alle vom DPC empfangenen Pakete (mit Ausnahme jener, die nicht von einer BIA konstruiert sind) enthalten einen BIA-Hardware-Identifizierungscode (die BIA-Identifizierung des Pakets), eine Folgenummer und einen MAC. Die GM bittet das MAC-Modul, den Paket-MAC zu validieren, und vergleicht dann die Folgenummer mit dem SNM (Sequence Number Module). Wenn die Kontrollen eine Übereinstimmung ergeben, leitet die GM das Paket zur Entschlüsselung an das MDM weiter. Wenn irgendeine der Kontrollen fehlschlagen sollte, gibt die GM eine Warnung aus, beendet die Verarbeitung des Pakets und sendet an die BIA eine Fehlermeldung zurück.

[0432] Derzeit sind die einzigen Nachrichtentypen, die nicht von einer BIA erstellt werden, die Aufforderungen betreffend gesicherte Faxdaten und elektronische Dokumentdaten.

1.5.5. Antwortpakete

[0433] Jedes vom DPC empfangene Paket kann einen optionalen Antwortschlüssel enthalten, der im verschlüsselten Biometrik-PIC-Block des Pakets gespeichert ist. Bevor das DPC auf eine Aufforderung antwortet, die einen Antwortschlüssel enthält, verschlüsselt es das Antwortpaket mit dem Antwortschlüssel. Es erzeugt auch einen MAC und fügt ihn an das Paket an.

[0434] Die einzige Ausnahme zur Verschlüsselung von Antwortpaketen betrifft Fehlermeldungen. Fehler werden niemals verschlüsselt und enthalten niemals vertrauliche Informationen. Die meisten Antwortpakte enthalten jedoch einen Status- oder Antwortcode, der anzeigen kann, ob die Anfrage erfolgreich war oder nicht. Wenn beispielsweise das DPC eine Kreditautorisierung verweigert, wird kein Fehlerpaket zurückgeschickt, sondern ein normales Transaktionsantwortpaket mit einem auf „fehlgeschlagen" eingestellten Antwortcode.

1.5.6. DPC-Verfahren

[0435] Das DPC wendet bei der Abwicklung von Anfragen bzw. Aufforderungen üblicherweise zwei Vorgangsweisen an.

1.5.6.1. Individuelle Identifizierungsprozedur

[0436] Für Aufforderungen, bei denen das DPC ein Individuum identifizieren muss, wendet das DPC die folgende Vorgangsweise an: Unter Einsatz des PIC-Codes sucht das DPC die IBD-Maschinen-Liste nach den Haupt- und Sicherungs-IBD-Maschinen ab, die für die Abwicklung der Identifizierungen des konkreten PIC-Codes zuständig sind. Als nächstes schickt das DPS die Identifizierungsaufforderung entweder an die Haupt- oder die Sicherungsmaschine (je nachdem welche von ihnen am wenigsten belastet ist). Die IBD-Maschine reagiert mit dem IBD-Eintrag für das Individuum oder mit einer „Individuum nicht gefunden"-Fehlermeldung.

[0437] Die IBD-Maschine ruft alle IBD-Einträge für den bestimmten PIC auf. Unter Verwendung einer proprietären biometrischen Hardwarevorrichtung vergleicht die IBD-Maschine die primäre biometrische Information jedes Eintrags mit der biometrischen Information des Individuums und gelangt zu einem Vergleichsscore, der die Ähnlichkeit der zwei biometrischen Informationen anzeigt. Wenn keine biometrische Information einen Vergleichswert aufweist, der nah genug ist, werden die Vergleiche mithilfe der zweiten biometrischen Eingabe wiederholt. Wenn keine der zweite biometrischen Eingabe einen ausreichend nahen Vergleichswert aufweist, schickt die IBD-Maschine eine „Individuum nicht gefunden"-Fehlermeldung zurück. Wenn nicht, gibt die IBD-Maschine den vollständigen IBD-Eintrag des Individuums aus, wobei Felder wie z. B. privater Code, Kontonummern, Titel usw. erhalten werden können.

1.5.6.2. Notfallsantwortprozedur

[0438] Bei Aufforderungen, die einen Kontoindex beinhalten, ist das DPC für Fälle zuständig, in denen das Individuum seinen Notfallskontoindex auswählt. Die die Aufforderung verarbeitende GM benachrichtigt die DPC-Support-Mitarbeiter sofort, gibt eine Warnung aus, und wenn das Antwortpaket einen Antwortcode aufweist, wird dieser auf „Notfall" gesetzt. Es ist die Verantwortung des Besitzers der BIA, die die Anfrage stellte,

auf einen „Notfalls"-Antwortcode zu achten und weiter Hilfestellung zu bieten, z. B. den Mechanismus des falschen Schirms (siehe Abschnitt über das Geldausgabeautomat-Endgerät ATM). Das DPC setzt auch im IBD-Eintrag des Individuums die Zahl der Notfalleinsätze entsprechend nach oben, jedes Mal wenn auf einen Notfallskontoindex zugegriffen wird.

1.5.7. Protokollanfragen

[0439] Die folgenden Abschnitte beschreiben jede Protokollanfrage/antwort und die vom DPC zu diesem Zweck ergriffenen Maßnahmen.

Die Liste der Protokollpakete

- Individuelle Identifizierung
- Transaktionsautorisierung
- Registrierung
- Kontozugriff
- Aussteller-Batch
- Sichere Faxvorlage
- Sichere Faxdaten
- Sichere Faxverfolgung
- Sicherer Faxabruf
- Sichere Faxabweisung
- Sichere Faxarchivierung
- Sichere Annahme des Faxvertrags
- Sichere Ablehnung des Faxvertrags
- Sichere Faxorganisationsänderung
- Elektronische Dokumentenvorlage
- Elektronische Dokumentenverfolgung
- Elektronischer Dokumentenabruf
- Elektronische Dokumentenabweisung
- Elektronische Dokumentenarchivierung
- Abruf archivierter elektronischer Dokumente
- Elektronische Signatur
- Verifizierung elektronischer Signatur
- Netzwerk-Akkreditiv

1.5.7.1. Individuelle Identifizierung
Individuelle Identifizierungsanfrage

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byt-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

MAC

Endgeräteteil: (nicht verwendet)

Individuelle Identifizierungsreaktion

verschlüsselter (Antwortschlüssel):

privater Codetext

individueller Name

biometrischer Identifizierungscode

MAC

[0440] Die individuelle Identifizierungsaufforderung enthält einen Biometrik-PIC-Block, den das DPC unter Anwendung der individuellen Identifizierungsprozedur zur Identifizierung des Individuums benutzt. Wenn das Individuum identifiziert ist, reagiert das DPC mit dem Namen des Individuums, seiner biometrischen Identifizierung und dem privaten Code. Ansonsten reagiert das DPC mit einer „unbekanntes Individuum"-Fehlermeldung.

1.5.7.2. Transaktionsautorisierung
Transaktionsautorisierungs-Anfrage

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenumer

verschlüsselter (DUKPT-Schlüssel) Biometrik-

PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

[optionaler 56-bit-Nachrichtschlüssel]

Kontoindex

Preis

Händleridentifizierung

[optionale Produktinformation in beliebigem

Format]

[optionaler Händlercode (Telefonnummer,

Kanalnummer + Zeit, Hostname)]

[optional Adressenzustellungsaufforderung]

MAC

Endgerätteil (nicht verwendet)

Transaktionsautorisierungs-Antwort

verschlüsselter (Antwortschlüssel):

privater Codetext

Autorisierungsantwort

Autorisierungsdetails (Autorisierungscode,

Transaktionsidentifizierung usw.)

[optionale individuelle Adresseninformation]

Antwortcode (fehlgeschlagen, OK, Notfall)

MAC

[0441] Es gibt zwei grundlegende Transaktionsautorisierungs-Subtypen: den Einzelhandel- und den Fern-Subtyp.

[0442] Für Einzelhandelautorisierungen identifiziert das DPC den Käufer mittels des Biometrik-PIC-Blocks der Aufforderung. Wenn das Individuum nicht identifiziert werden kann, antwortet das DPC mit einer „unbekanntes Individuum"-Fehlermeldung.

[0443] Als nächstes sendet das DPS eine externe Autorisierungsaufforderung (mittels Gutschrift auf das Finanzkonto des BIA-Besitzers und Lastschrift auf das Finanzkonto des Individuums) an eine von mehreren bestehenden Finanzautorisierungsdienste, wobei dies von der Art der jeweiligen Finanzkonten abhängt (z. B. Visa™ oder American Express™). Wenn der externe Finanzautorisierungsdienst die Transaktion genehmigt, sendet das DPC die externen Autorisierungscodes und anschließend einen „OK"-Antwortcode an die BIA zurück.

[0444] Andernfalls gibt das DPC in seiner Antwort den Grund dafür an, warum die Autorisierung abgelehnt wurde, und setzt den Antwortcode auf „fehlgeschlagen". In beiden Fällen ist der private Code des Individuums in der Reaktion des DPC beinhaltet.

[0445] Wenn das DPC mittels des Kontoindex der Aufforderung das Finanzkonto des Individuums begutachtet, kann das ausgewählte Konto das „Notfalls"-Konto sein. Wenn dies eintritt, ermöglicht das DPC den Start der Notfallsantwortprozedur. Die externe Autorisierung findet aber trotzdem statt.

[0446] Die Fernautorisierung erfolgt durch Telefon-, Versandhaus- oder Kabel-TV-Händler. Das DPC wickelt Fernautorisierungen mit den folgenden Ausnahmen in gleicher Weise wie eine Einzelhandelsautorisierung ab:

i) Fernautorisierungen enthalten einen Fernhändler-Code, den das DPC mit der Fernhändler-Datenbank vergleicht, um zu validieren, ob die Händleridentifizierung des Pakets mit der in der Datenbank gespeicherten übereinstimmt. Außerdem ist das die Gutschrift erhaltende Finanzkonto das Konto des Fernhändlers, nicht das Konto des BIA-Vorrichtungsbesitzers.

ii) Außerdem sind BIA-Vorrichtungen, die Fernautorisierungen erstellen, zumeist persönliche BIAs. Das DPC überprüft die biometrische Identifizierung des identifizierten Individuums und vergleicht sie mit der AID (Authorized Individual Database)-Liste von Individuen, die die BIA verwenden dürfen. Wenn dem Individuum keine Genehmigung erteilt wurde, die Vorrichtung zu verwenden, verweigert das DPC die Autorisierungsanfrage.

iii) Schließlich kann das Autorisierungspaket einen „Adressenzustellungs"-Indikator enthalten. Dieser Indikator informiert das DPC, dass die Adresse des Individuums im Antwortpaket enthalten sein soll; er wird üblicherweise nur für Versandhauseinkäufe verwendet.

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

1000-Byte-Primärbiometrik

1000-Byte-Sekundärbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

56-Bit-Nachrichtenschlüssel

MAC

Endgerätteil:

verschlüsselter (Nachrichtenschlüssel):

Name

Adresse

Postleitzahl

privater Code

Finanzkontoliste (Kontoindexcode, Kontonummer)

Notfallskonto (Kontoindexcode, Kontonummer)

Titelliste (Titelindexcode, Titelname)

Registrierungsantwort

Statuscode

verschlüsselter (Nachrichtenschlüssel):

privater Codetext

PIC

biometrischer Identifizierungscode

Liste von DPC-ausgewählten PICs

(wenn ursprüngliche PIC-Wahl

abgelehnt wird)

Statuscode (OK, abgelehnt)

MAC

[0447] Individuen registrieren sich im DPC über ein BRT (Biometric Registration Terminal). Das BRT sendet dem DPC ein Registrierungspaket zu, das primäre und sekundäre biometrische Informationen, den PIC sowie zusätzliche Daten wie etwa Name, Adresse, Kontoliste, privaten Code und Notfallcode des Individuums enthält. Gegebenenfalls kann das Individuum eine E-Mail-Adresse, eine Titelliste mit Titeln und den Titelindexcode sowie eine Sozialversicherungsnummer (SSN, Social Security Number) angeben. Das Individuum kann seinen eigenen PIC auswählen oder ihn vom System auswählen lassen. In einem Modifikationsschritt können zuvor eingegebene Daten modifiziert oder gelöscht werden.

[0448] Es dient immer nur jeweils ein DPC-Standort als Registrierungsstelle, um auf diese Weise die Implementierung zu vereinfachen. Die RegistrierungsAnfragepakete, die Nicht-Registrierungs-DPC-Stellen erhalten, werden an die aktuelle Registrierungsstelle weitergeleitet. Die Registrierungs-DPC-Stelle führt die gesamte Registrierungskontrolle durch, weist den IBD-Maschinen IBD-Einträge zu und ist für die dezentrale Transaktion zuständig, die für das Update aller anderen DPC-Stellen notwendig ist.

[0449] Die Registrierungs-DPC-Stelle wählt den PIC-Code für Registrierungsanfragen, die keinen angegeben haben, speichert den IBD-Eintrag auf der Haupt- und der Sicherungs-IBD-Maschine (angeführt in der PIC-Gruppen-Liste) und überprüft die PIC- und biometrische Eignung des Registrierungspakets, bevor es die dezentrale Transaktion startet, um alle anderen DPC-Stellen zu updaten.

[0450] Das DPC führt einen Duplikatvergleich des PIC und der biometrischen Probe durch, bei dem die biometrische Probe und der PIC (während des Registrierungsschritts erhalten) mit allen zuvor registrierten biometrischen Eingaben verglichen werden, die derzeit mit dem identischen PIC assoziiert sind. Das DPC kann die Registrierung aus den folgenden Gründen ablehnen: Der PIC ist zu populär, oder die biometrischen Proben ähneln anderen unter dem ausgewählten PIC gespeicherten biometrischen Proben zu stark. Um das Individuum bei der Auswahl eines geeigneten PIC zu unterstützen, erstellt das DPC eine kurze Liste von PICs, für die die Registrierung garantiert ist, d. h. die es über eine bestimmte Zeit reserviert. Das BRT fordert dann das Individuum auf, einen neuen PIC aus der Liste passender PICs auszuwählen.

1.5.7.4. Kontozugriff
Kontozugriffanfrage

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPIT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

[optionaler 56-bit-Nachrichtenschlüssel]

Kontoindex

MAC

Endgerätteil (nicht verwendet)

Kontozugriffsantwort

verschlüsselter (Nachrichtenschlüssel):

privater Codetext

[optional PIC]

Kontonummer

Antwortcode (fehlgeschlagen, OK, Notfall)

MAC

[0451] Die Kontozugriffsanfrage bietet den Benutzern von mit BIA ausgestatteten Geldausgabeautomaten die Möglichkeit der sichereren und bequemeren Identifizierung gegenüber dem Geldausgabeautomaten.

[0452] Die GM identifiziert das Individuum durch den Biometrik-PIC des Pakets und bedient sich des angegebenen Kontoindex, um die abzurufende Kontonummer auszuwählen.

[0453] Wenn die GM die Kontonummer mittels des Kontoindex der Anfrage nachsieht, kann das ausgewählte Konto das Notfallskonto sein. Wenn dies der Fall ist, folgt die GM der Notfallsantwortprozedur.

1.5.7.5. Aussteller-Batch
Aussteller-Batchanfrage

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

56-Bit-Nachrichtenschlüssel

Ausstellercode

MAC

Endgerätteil:

verschlüsselte (Nachrichtenschlüssel) Batchliste:

hinzufügen <biometrische Identifikation> <Kontoindex> <Finanzkonto>

[<Notfallskennung>]

entfernen <biometrische Identifikation> <Kontoindex> <Finanzkonto>

Ausstellerstapelantwort

verschlüsselt (Antwortschlüssel):

privater Codetext

Antwortcode (fehlgeschlagen, OK, Notfall)

MAC

verschlüsselte (Nachrichtenschlüssel) „fehlgeschlagen"-Liste:

fehlgeschlagen <Befehl> <Code>

.....

[0454] Die Aussteller-Batchanfrage ermöglicht es, einer ausstellenden Bank oder anderen Stelle, Routinewartungen in der IBD vorzunehmen. Das DPC gibt eine Warnung infolge des Verstoßes gegen die Sicherheitsvorschriften aus, wenn es Aussteller-Batchanfragen von Nicht-Aussteller-BIAs erhält, und weigert sich auch, dieser Anfrage nachzukommen.

[0455] Das DPC identifiziert das die Batchanfrage vorlegende Individuum, indem die individuelle Identifizierungsprozedur befolgt wird. Das DPC überprüft dann, dass das Individuum in der AID registriert ist, um die im absendenden Ausstellerendgerät eingebettete BIA zu verwenden.

[0456] Das DPC verwendet auch den Ausstellercode in der Anfrage, um die Vorrichtungs-Besitzer-Identifikation in der Ausstellerdatenbank nachzusehen, und vergleicht sie mit der in der VAD (Valid Apparatus Database) gespeicherten Vorrichtungs-Besitzer-Identifikation, um sicherzustellen, dass der Ausstellercode nicht gefälscht ist.

[0457] Das DPC führt dann die Hinzufügungs- und Löschbefehle in der mittels Nachrichtenschlüssel verschlüsselten Batchliste aus. Die Batchliste ist mit neuer Zeile getrennte Liste von Befehlen. Es gibt die folgenden gültigen Befehle:
hinzufügen <biometrische Identifikation> <Kontoindex> <Finanzkonto>
[<Notfallskennung>]
entfernen <biometrische Identifikation> <Kontoindex> <Finanzkonto>

[0458] Der Befehl „Hinzufügen" fügt das Konto zu der Kontoliste im angeführten Kontoindex hinzu. Die optionale Notfallskennung zeigt an, ob der bestimmte Kontoindex als Notfallskonto des Individuums behandelt wird. Wenn das aktuell in der Kontoliste gespeicherte Finanzkonto nicht dem Aussteller zuzurechnen ist, ist der Befehl erfolglos. Dieses Fehlschlagen verhindert, dass eine Bank Finanzkonten von Kunden einer anderen Bank ohne Wissen oder Genehmigung des Individuums hinzufügt oder entfernt.

[0459] Der Befehl „Entfernen" löscht das im angegebenen Kontoindex in der Kontoliste gespeicherte Finanzkonto des Individuums. Wenn das aktuell in der Kontoliste gespeicherte Finanzkonto nicht mit dem Konto übereinstimmt, auf das der Aussteller zugreifen möchte, ist der Befehl erfolglos.

[0460] Für jeden Befehl im Stapel, der nicht korrekt ausgeführt werden konnte, gibt die GM eine Warnung aufgrund eines Verstoßes gegen die Sicherheitsvorschriften aus, und fügt der „fehlgeschlagen"-Liste der Antwort einen Eintrag an. Dieser Eintrag enthält den Text für den Befehl und den Fehlercode.

1.5.7.6. Sichere Faxvorlage

Anfrage zur sicheren Faxvorlage

BIA-Teil:
4-Byte-BIA-Identifizierung
4-Byte-Folgenummer
verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:
300-Byte-Autorisierungsbiometrik
4-12-stelliger PIC
56-Bit-Antwortschlüssel
56-Bit-Nachrichtenschlüssel
Sicherheitsmodus (ungesichert, Absender-gesichert, gesichert, gesichert-vertraulich)
Absendertitelindexcode
Absenderfaxnummer
Absenderfaxdurchwahl
Empfängerliste
[optionaler Archivfaxindikator]
[optionaler Vertrags/Vereinbarungsindikator]
Endgerätteil (nicht verwendet)

Antwort auf sichere Faxvorlage

verschlüsselt (Nachrichtenschlüssel):

privater Codetext

Faxverfolgungsnummer

MAC

[0461] Wenn das DPC eine Anfrage zur sicheren Faxvorlage erhält, identifiziert es das Individuum anhand des Biometrie-PIC der Anfrage, indem die individuelle Identifizierungsprozedur befolgt wird. Diese Identifizierung wird gemeinsam mit dem durch den Titelindexcode beschriebenen Titel des Individuums den Empfängern vorgelegt, so dass der Absender der Faxnachricht immer zuverlässig identifiziert wird.

[0462] Das DPC erstellt zwecks Rückverfolgung eine Verfolgungsnummer und speichert diese, die biometrische Identifizierung des Absenders, den Sicherheitsmodus und den Nachrichtenschlüssel im neu angelegten EDD-Dokumenteneintrag. Für jeden Empfänger in der Empfängerliste erstellt das DPC auch einen Empfängereintrag. Das DPC wartet dann auf das sendende Faxgerät, um die unter dem Nachrichtenschlüssel verschlüs-

selten Faxdaten zu übermitteln.

[0463] Wenn die Anfrage einen „Archivfax"- oder „Vertrags/Vereinbarungs"-Indikator enthält, stellt die EDD eine Kopie der Dokumenten- und Empfängereinträge in die Archivdatenbank. Alle nachfolgenden Aktualisierungen dieser Aufzeichnungen werden auch in den archivierten Versionen vorgenommen.

[0464] Die Faxdaten werden in einem getrennten Schritt übermittelt, so dass der Absender, falls er einen Fehler bei der Eingabe seiner biometrischen Daten und seines PIC macht, vom System verständigt wird, bevor er unnötigerweise das Dokument in das Faxgerät einlegt.

1.5.7.7. Sichere Faxdaten
Anfrage zu sicheren Faxdaten

BIA-Teil (nicht verwendet)

Endgerätteil:

Faxverfolgungsnummer

verschlüsselt (Nachrichtenschlüssel):

Faxbilddaten

Antwort auf sichere Faxdaten

Status (unvollständig, OK)

[0465] Aufgrund der Anfrage zu sicheren Faxdaten kann ein sicheres Faxgerät das Faxbild an das DPC senden, damit es an den oder die zuvor angegebenen Empfänger zugestellt werden kann. Diese Anfrage bzw. Aufforderung umfasst keine biometrische Identifizierung und beruht stattdessen auf dem geheimen Nachrichtenschlüssel, um das Bild sicher zu übertragen.

[0466] Die Faxbilddaten werden durch den Nachrichtenschlüssel verschlüsselt, der durch die Anfrage zur sicheren Faxvorlage registriert wird. Sobald das DPC das gesamte Fax empfangen hat, schickt es eine Meldung über den Empfang eines sicheren Faxes an die Faxnummern der Empfänger. Das DPC ruft die Liste von Empfängern auf, indem die EDD nach allen Empfängereinträgen durchsucht wird, die die Faxverfolgungsnummer enthalten. Der Empfängereintrag enthält die Zielfaxnummer und gegebenenfalls eine Nebenstelle. Nach dem Absenden der Mitteilung über eine eingetroffene Faxnachricht aktualisiert das DPC das Zustellungsstatusfeld jedes Empfängereintrags auf „benachrichtigt". Folgendes ist zu beachten: Wenn die Zielfaxnummer besetzt ist, markiert das DPC das Zustellungsstatusfeld als „besetzt" und versucht in regelmäßigen Abständen die Mitteilung erneut zu schicken (d. h. alle 10 Minuten), bis die Übertragung funktioniert; zu diesem Zeitpunkt wird das Statusfeld auf „benachrichtigt" umgeändert.

[0467] Die Ankunftsmitteilung ist folgendermaßen aufgebaut:
Mitteilung über das Eintreffen sicherer Faxnachrichten (Faxnachricht)
Absendername, Firma, Titel und Faxnummer
Faxverfolgungsnummer
Anweisungen über das Herunterladen des Faxes

[0468] Das DPC faxt dem Absender erst dann eine Statusmitteilung zu, wenn alle Empfänger das Fax entweder abgerufen oder abgewiesen haben. Der Absender kann beim DPC mittels der Anfrage zur sicheren Faxverfolgung (siehe unten) nachfragen, um den aktuellen Status aller Empfänger zu erfahren.

[0469] Die Statusmitteilung ist folgendermaßen aufgebaut:
Mitteilung über den Status sicherer Faxnachrichten (Faxnachricht)
Absendername, Unternehmen, Titel und Faxnummer
Faxverfolgungsnummer
Empfängerliste einschließlich:
Name, Unternehmen, Titel und Faxnummer
Zustelldatum und -status
Vertrags/Vereinbarungsstatus

[0470] Das DPC findet Informationen über das Unternehmen und den Titel jedes Individuums in der EDD-Organisationstabelle.

[0471] Im Falle von Individuen, die nicht im System registriert sind und daher keine sicheren Faxe empfangen können, oder von Nicht-Empfänger-gesicherten Modi schickt ihnen das DPC keine Mitteilung über die Ankunft eines gesicherten Faxes. Stattdessen schickt ihnen das DPC die Faxnachricht direkt. Wenn die Faxleitung besetzt ist, ersucht es das DPC alle 10 Minuten erneut, bis das Fax erfolgreich zugestellt werden kann.

1.5.7.8. Sichere Faxverfolgung
Anfrage zur sicheren Faxverfolgung

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrie-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

56-Bit-Nachrichtenschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil (nicht verwendet)

Antwort auf sichere Faxverfolgung

verschlüsselt (Nachrichtenschlüssel):

privater Codetext

Message Digest für Faxbild-Verfolgungsantwort

Statuscode (OK, fehlgeschlagen)

MAC

Faxbild für Empfängerstatusliste

[0472] Das DPC reagiert auf die Anfrage betreffend die Verfolgung sicherer Faxnachrichten, indem alle EDD-Empfängereinträge aufgerufen werden und eine Faxnachricht erstellt wird, um die Einträge anzuzeigen. Wenn das die Verfolgungsanfrage richtende Individuum nicht der Absender des Faxdokuments ist, setzt das DPC den Statuscode auf „fehlgeschlagen" und setzt in der Antwort ein leeres Fax ein.

[0473] Das Verfolgungsantwort-Fax enthält Informationen über den Status der Zustellung der Faxmitteilung an jeden Empfänger. Dieses Fax enthält Statusinformationen wie etwa „Leitung besetzt", „Faxankunftsmitteilung gesendet", „Fax gesendet", „Fax abgewiesen", „Vertrag angenommen" usw.

[0474] Die Verfolgungsmitteilung ist folgendermaßen aufgebaut:
Mitteilung über die Verfolgung sicherer Faxnachrichten (Faxnachricht)
Absendername, Unternehmen, Titel und Faxnummer
Faxverfolgungsnummer
Empfängerliste einschließlich:
Name, Unternehmen, Titel und Faxnummer
Zustellungsdatum und -status

Vertragsstatus

1.5.7.9. Sicherer Faxabruf
Anfrage zum sicheren Faxabruf

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf sicheren Faxabruf

verschlüsselt (Nachrichtenschlüssel):

privater Code

56-Bit-Nachrichtenschlüssel

Status (unvollständig, OK, ungültiger Empfänger)

Message Digest für Faxbild

MAC

verschlüsselt (Nachrichtenschlüssel):

Faxbild

[0475] Das DPC bedient sich des Biometrik-PIC, um das die Abrufabfrage stellende Individuum zu identifizieren, indem die individuelle Identifizierungsprozedur befolgt wird. Wenn kein EDD-Empfängerintrag für das Individuum und das angeführte Fax besteht, reagiert das DPC mit dem Status „ungültiger Empfänger".

[0476] Das DPC ruft das verschlüsselte Faxbild aus dem EDD-Dokumenteneintrag mit der korrekten Faxverfolgungsnummer und biometrischen Identifizierung ab und sendet es an die anfragende Person zurück.

[0477] Das Faxbild enthält ein Deckblatt, auf dem zu sehen ist, ob das Fax ein Vertrag/eine Vereinbarung ist; ferner enthält das Deckblatt den Namen des Absenders, sein Unternehmen, seinen Titel, seine Faxnummer und seine Durchwahl.

[0478] Wenn der letzte Empfänger das Fax entweder empfangen oder abgelehnt hat, faxt das DPC eine Statusmitteilung (siehe obiges Kapitel über sichere Faxdaten) an den Absender der Faxnachricht und nennt dann einen konfigurierbaren Zeitraum, in dem die Dokumenten- und Empfängereinträge aus der EDD gelöscht werden. Der Zeitraum soll den Empfängern ausreichend Zeit geben, um sich zu entscheiden, ob sie das Fax archivieren wollen oder nicht.

1.5.7.10. Sichere Faxabweisung
Anfrage zur sicheren Faxabweisung

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf sichere Faxabweisung

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiger Empfänger)

MAC

[0479] Das DPC bedient sich des Biometrik-PIC, um das Individuum zu identifizieren, das die Anfrage zur sicheren Faxabweisung stellt. Das DPC findet den EDD-Empfängereintrag (der Schlüssel dafür sind die Faxverfolgungsnummer der Anfrage und die biometrischen Identifizierung des Individuums). Wenn keine Eintragung gefunden wird, schlägt die Anfrage mit einer „ungültiger Empfänger"-Statusmeldung fehl.

[0480] Wenn der letzte Empfänger das Fax entweder erhalten oder abgewiesen hat, faxt das DPC eine Statusmeldung (siehe obiges Kapitel über sichere Faxdaten) an das Faxgerät des Absenders und nennt dann einen konfigurierbaren Zeitraum, in dem die Fax- und Verfolgungseinträge aus der EDD gelöscht werden. Der Zeitraum soll den Empfängern ausreichend Zeit geben, um sich zu entscheiden, ob sie das Fax archivieren wollen oder nicht.

1.5.7.11. Sichere Faxarchivierung
Anfrage zu sicherer Faxarchivieriung

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf sichere Faxarchivierung

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiges Individuum)

MAC

[0481] Das DPC bedient sich des Biometrik-PIC, um das die Anfrage betreffend sichere Faxarchivierung richtende Individuum zu identifizieren. Das DPC findet den EDD-Empfängereintrag, dessen Schlüssel die Faxverfolgungsnummer und die biometrische Identifizierung des Individuums ist. Wenn der Eintrag nicht auffindbar ist und das Individuum nicht der Absender oder einer der Empfänger ist, schlägt die Anfrage fehl (ihr Status ist der des „ungültigen Individuums"). Andernfalls kopiert das DPC die Dokumenten- und Empfängereinträge in die EDD-Archivdatenbank. Alle nachfolgenden Veränderungen dieser Einträge werden auch in die archivierten Versionen kopiert.

1.5.7.12. Annahme sicherer Faxaufträge
Anfrage zur Annahme sicherer Faxaufträge

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Annahme sicherer Faxaufträge

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiger Empfänger)

MAC

[0482] Das DPC verwendet den Biometrik-PIC, um das die Anfrage bezüglich der Vertragsannahme richtende Individuum zu identifizieren. Das DPC findet den EDD-Empfängereintrag, dessen Schlüssel die Faxverfolgungsnummer der Anfrage und die biometrische Identifizierung des Individuums ist. Wenn der Eintrag nicht auffindbar ist, schlägt die Anfrage fehl (ihr Status ist der des „ungültigen Empfängers"). Andernfalls aktualisiert das DPC das Vertragsstatusfeld des Empfängereintrags auf „angenommen" und erstellt eine an den Faxabsender geschickte Statusmitteilung (siehe obiges Kapitel über Faxdaten).

1.5.7.13. Ablehnung sicherer Faxverträge
Anfrage zur Ablehnung sicherer Faxverträge

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Faxverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Ablehnung sicherer Faxverträge

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiger Empfänger)

MAC

[0483] Das DPC verwendet den Biometrik-PIC, um das die Anfrage bezüglich der Vertragsablehnung richtende Individuum zu identifizieren. Das DPC findet den EDD-Empfängereintrag, dessen Schlüssel die Faxverfolgungsnummer der Anfrage und die biometrische Identifizierung des Individuums ist. Wenn der Eintrag nicht auffindbar ist, schlägt die Anfrage fehl (ihr Status ist der des „ungültigen Empfängers"). Andernfalls aktualisiert das DPC das Vertragsstatusfeld des Empfängereintrags auf „abgelehnt" und erstellt eine an den Faxabsender geschickte Statusmitteilung (siehe obiges Kapitel über Faxdaten).

1.5.7.14. Sichere Faxorganisationsveränderung

Sichere Faxorganisationsveränderung (sichere Faxnachricht)
Absendername, Unternehmen, Titel und Faxnummer
Liste organisatorischer Veränderungen

[0484] Organisationsveränderungen werden dem DPC mittels einer sicheren Faxnachricht mitgeteilt. Ein Kundensupport-Techniker gibt die in der Faxmitteilung angeführten gewünschten Veränderungen ein und verifiziert dabei, dass das die Anfrage stellende Individuum Individuen für diese bestimmte Firma registrieren kann. Da das Fax eine sichere Faxmitteilung ist, wurde die Identität des Absenders wie auch sein Titel bereits ermittelt.

1.5.7.15. Elektronische Dokumentenvorlage
Anfrage zur elektronischen Dokumentenvorlage

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

56-Bit-Nachrichtenschlüssel

Empfängerliste

MAC

Endgerätteil: (nicht verwendet)

Antwort zur elektronischen Dokumentenvorlage

verschlüsselt (Antwortschlüssel):

privater Code

Verfolgungsnummer

Statuscode (OK, ungültiger Empfänger)

MAC

[0485] Wenn das DPC eine Anfrage zur elektronischen Dokumentenvorlage erhält, identifiziert es das Individuum, indem die individuelle Identifizierungsprozedur befolgt wird.

[0486] Das DPC legt dann einen EDD-Dokumenteneintrag an und weist ihm eine eindeutige Verfolgungsnummer zu. Das DPC initialisiert den Absenderidentifizierungscode des Eintrags, damit er als biometrischer Identifizierungscode des identifizierten Individuums dient, und initialisiert auch den Nachrichtenschlüssel, damit er in der Anfrage als Nachrichtenschlüssel dient.

[0487] Als nächstes sucht das DPC die individuelle biometrische Datenbank hinsichtlich des Empfängers ab und legt für jeden einen EDD-Empfängereintrag an. Jeder Eintrag wird mit der Verfolgungsnummer, dem biometrischen Identifizierungscode des Empfängers und dem Zustellstatus „unvollständig" initialisiert. Wenn Empfänger nicht auffindbar sind, antwortet das DPC mit dem Status „ungültiger Empfänger".

1.5.7.16. Elektronische Dokumentdaten
Anfrage zu elektronischen Dokumentdaten

BIA-Teil: (nicht verwendet)

Endgerätteil:

Verfolgungsnummer

Befehl (entweder Abbruch oder Daten)

[optional Message Offset]

Abschlussindikator

verschlüsselt (Nachrichtenschlüssel):

Nachrichtenkörper

Antwort auf elektronische Dokumentdaten

Status (unvollständig, OK)

[0488] Die Anfrage zu elektronischen Dokumentdaten ermöglicht es einem Individuum, den Dokumenttext (in einem oder mehreren Teilen) an die EDD zu schicken, damit er an den bzw. die Empfänger zugestellt werden kann. Diese Anfrage umfasst keinerlei biometrische Identifizierung; stattdessen beruht sie auf dem geheimen Nachrichtenschlüssel, um den Dokumenttext sicher übertragen zu können.

[0489] Man nimmt an, dass der Anfragetext durch den im EDD-Dokumenteneintrag gespeicherten Nachrichtenschlüssel verschlüsselt und an den bereits im Eintrag gespeicherten Dokumenttext angefügt ist.

[0490] Wenn die EDD ein Paket mit dem Indikator „Dokument vollständig" erhält, weiß sie, dass der Absender die Übertragung des Dokuments abgeschlossen hat. Die EDD sendet nun eine Ankunftsmitteilung an alle Empfänger des Dokuments (über Internet-E-Mail), um sie davon zu informieren, dass auf sie ein Dokument wartet.

[0491] Die Ankunftsmitteilung ist wie folgt aufgebaut:
Mitteilung über die Ankunft elektronischer Dokumente (Internet-E-Mail-Nachricht)
Absendername, Unternehmen, Titel und E-Mail-Adresse
Verfolgungsnummer
Anweisungen über den Empfang des elektronischen Dokuments

[0492] Die EDD aktualisiert auch den Status des EDD-Empfängereintrags auf „benachrichtigt". Wenn alle Empfänger das elektronische Dokument entweder abgerufen oder abgewiesen haben, sendet das DPC über Internet-E-Mail eine Statusmitteilung an den Dokumenterststeller.

[0493] Die Statusmitteilung ist wie folgt aufgebaut:
Mitteilung über den elektronischen Dokumentstatus (Internet-E-Mail-Nachricht)
Absendername, Unternehmen, Titel und E-Mail-Adresse
Verfolgungsnummer
Empfängerliste einschließlich:
Name, Unternehmen, Titel, E-Mail-Adrsse
Zustellungsdatum und -status

[0494] Das DPC findet Informationen bezüglich des Unternehmens und Titels des Individuums in der EDD-Organisationstabelle.

1.5.7.17. Abruf elektronischer Dokumente
Anfrage zum Abruf elektronischer Dokumente

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Verfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Abruf elektronischer Dokumente

verschlüsselt (Antwortschlüssel):

privater Code

56-Bit-Nachrichtenschlüssel

Status (unvollständig, OK, ungültiger Empfänger)

MAC

verschlüsselt (Nachrichtenschlüssel):

Dokumenttext

[0495] Mithilfe des Biometrik-PIC kann das DPC das die Anfrage zum elektronischen Dokumentenabruf richtende Individuum identifizieren, indem die folgende Identifizierungsprozedur befolgt wird.

[0496] Das DPC findet als nächstes den EDD-Empfängereintrag, dessen Schlüssel die Verfolgungsnummer und biometrische Identifizierung des Individuums ist.

[0497] Wenn kein Eintrag auffindbar ist, schlägt die Anfrage mit dem Status „ungültiger Empfänger" fehl. Andernfalls sendet das DPC den Nachrichtenschlüssel des Dokuments und das Dokument (nach wie vor durch den Nachrichtenschlüssel verschlüsselt) an die anfragende Person.

[0498] Das EDD ändert dann den Status des EDD-Empfängereintrags auf „abgerufen". Wenn alle Empfänger das Dokument entweder abgerufen oder abgewiesen haben, übermittelt das DPC über Internet-E-Mail eine Statusmitteilung an den Dokumentenersteller (siehe obiges Kapitel über elektronische Dokumentdaten) und setzt die Entfernung der Dokumenten- und Empfängereinträge fest (siehe obiges Kapitel über sicheren Faxabruf).

1.5.7.18. Abweisung elektronischer Dokumente
Anfrage zur Abweisung elektronischer Dokumente

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Nachrichtenverfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Abweisung elektronischer Dokumente

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiger Empfänger)

MAC

[0499] Mithilfe des Biometrik-PIC kann das DPC das Individuum identifizieren, das die Anfrage zur Abweisung elektronischer Dokumente richtet. Das DPC findet als nächstes den EDD-Empfängereintrag, dessen Schlüssel die Verfolgungsnummer und die biometrische Identifizierung des Individuums ist. Wenn kein Eintrag auffindbar ist, schlägt die Anfrage mit dem Status „ungültiger Empfänger" fehlt.

[0500] Die EDD ändert den Status des EDD-Empfängereintrags auf „abgewiesen". Dann führt das DPC die gleiche Benachrichtigungs- und Löschungsprozedur aus, die im obigen Kapitel über den Abruf elektronischer Dokumente beschrieben ist.

1.5.7.19. Archivierung elektronischer Dokumente
Anfrage zur Archivierung elektronischer Dokumente

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Verfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Archivierung elektronischer Dokumente

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiges Individuum)

MAC

[0501] Das DPC bedient sich des Biometrik-PIC, um das Individuum zu identifizieren, das die Anfrage zur Archivierung elektronischer Dokumente stellte. Das DPC findet dann den EDD-Empfängereintrag, dessen Schlüssel die Verfolgungsnummer der Anfrage und die biometrische Identifizierung des Individuums ist. Wenn der Eintrag nicht auffindbar ist und das Individuum nicht der Absender oder einer der Empfänger ist, schlägt die Anfrage mit dem Status „ungültiges Individuum" fehl. Andernfalls kopiert das DPC die Dokumenten- und Empfängereinträge in die EDD-Archivdatenbank. Alle späteren Änderungen dieser Einträge werden auch in die archivierten Versionen kopiert.

1.5.7.20. Abruf archivierter elektronischer Dokumente
Anfrage zum Abruf archivierter elektronischer Dokumente

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

optional Titelindexcode, Absenderfaxnummer und –durchwahl

Verfolgungsnummer

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Abruf archivierter elektronischer Dokumente

verschlüsselt (Antwortschlüssel):

privater Code

Statuscode (OK, ungültiges Individuum)

MAC

[0502] Das DPC kann eine Anfrage zum Abruf archivierter elektronischer Dokumente entweder von eine Sicherenfaxendgerät oder einem zertifizierten E-Mail-Endgerät empfangen. Das DPC wendet die Vorgangsweise der individuellen Identifizierung an, um das Individuum zu bestimmen, das die Archivabrufanfrage stellt. Das Individuum muss entweder der Absender oder einer der Empfänger sein; andernfalls lehnt das DPC die Anfrage ab, indem der Statuscode auf „ungültiges Individuum" gesetzt wird. Wenn jedoch das archivierte Dokument ein Fax ist, das mit einem Unternehmenstitel übermittelt wurde, erlaubt es das DPC zusätzlichen Individuen, deren Titel in der Firmenhierarchie höher sind, das archivierte Dokument ebenfalls abzurufen.

[0503] Das EDD verwaltet eine Archivdatenbank (indexiert nach ursprünglicher Dokumentenverfolgungsnummer und gespeichert auf Offline-Medien wie z. B. CD-ROMs und Bändern, so dass die Suche nach dem archivierten Dokument möglicherweise viel Zeit in Anspruch nehmen kann). In der Folge schickt das DPC das

archivierte Dokument nicht sofort zurück, sondern informiert das die Anfrage richtende Individuum, dass das DPC mit der Suche begonnen hat. Zu einem späteren Zeitpunkt – wenn die Suche abgeschlossen ist – benachrichtigt das DPC die die Anfrage richtende Person, dass das archivierte Dokument nun über die herkömmlichen Mechanismen der Dokumentankunftsverständigung (entweder Fax oder E-Mail, je nach dem Format des Originaldokuments) nunmehr abrufbar ist.

[0504] Das DPC legt einen EDD-Archivierungsanfrage-Eintrag an, um Informationen über das anfragende Individuum zu speichern, so dass bei Abschluss der Suche das DPC noch weiß, an wen das Dokument zu schicken ist.

1.5.7.21. Elektronische Signatur
Anfrage zur elektronischen Signatur

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Dokumentname

Dokument-MD5-Berechnung

MAC

Endgerätteil: (nicht verwendet)

Antwort auf elektronische Signatur

verschlüsselt (Antwortschlüssel):

privater Codetext

Signaturstring

MAC

[0505] Zur Abwicklung von Anfragen bezüglich elektronischer Signaturen führt das DPC zunächst eine biometrische Identifizierung unter Verwendung des Biometrik-PIC durch. Dann legt das DPC einen ESD-Eintrag an, weist ihm einen eindeutigen Signaturidentifizierungscode zu und setzt das Signaturfeld des Eintrags auf die elektronische Signatur in der Anfrage. Das DPC schickt dann einen Signaturstring zurück, der zur späteren Verifizierung vorgelegt werden kann:
„<Dr. Bunsen Honeydew> <Explosionen im Labor> 5/17/95 13:00 PST 950517000102"

1.5.7.22. Verifizierung elektronischer Signaturen
Anfrage zur Verifizierung elektronischer Signaturen

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Signaturstring

MAC

Endgerätteil: (nicht verwendet)

Antwort auf Verifizierung elektronischer Signaturen

verschlüsselt (Antwortschlüssel):

privater Codetext

Signaturstring

Status (verifiziert, fehlgeschlagen)

MAC

[0506] Das DPC nimmt eine biometrische Identifizierung vor, extrahiert den Signaturverfolgungscode aus dem Signaturstring, ruft den angegebenen ESD-Eintrag ab und verifiziert, dass er mit dem Signaturstring übereinstimmt. Das DPC sendet den privaten Code und das Ergebnis des Signaturvergleichs zurück.

1.5.7.23. Netzwerk-Akkreditiv
Anfrage zum Netzwerk-Akkreditiv

BIA-Teil:

4-Byte-BIA-Identifizierung

4-Byte-Folgenummer

verschlüsselter (DUKPT-Schlüssel) Biometrik-PIC-Block:

300-Byte-Autorisierungsbiometrik

4-12-stelliger PIC

56-Bit-Antwortschlüssel

Kontoindex

Bankleitzahl

Bankhostname

Endgerät.Anschluss und Bank.Anschluss (TCP/IP-Adressen)

MAC

Antwort auf Netzwerk-Akkreditiv

verschlüsselt (Antwortschlüssel):

privater Code

signiert (DPC-Privatschlüssel):

Akkreditiv (Zeit, Konto, Endgerät.Anschluss, Bank.Anschluss)

Public Key der Bank

Statuscode (OK, fehlgeschlagen)

MAC

[0507] Das DC identifiziert das den Anfrage-Biometrik-PIC verwendende Individuum und ruft das im angegebenen Index gespeicherte Finanzkonto des Individuums ab. Wenn der Kontoindex das Notfallskonto ist, wird der Statuscode der Netzwerk-Credential-Antwort auf „fehlgeschlagen" gesetzt und kein Akkreditiv erzeugt.

[0508] Das DPC erstellt das Akkreditiv unter Heranziehung der aktuellen Zeit, des abgerufenen Finanzkontos sowie der TCP/IP-Adressen des Endgeräts und der Bank. Das DPC wendet dann Public Key-Verschlüsselung an, um das Akkreditiv mit seinem privaten Schlüssel zu signieren.

[0509] Die Antwort enthält auch den Public Key der Bank, den das DPC aus der Fernhändlerdatenbank abruft.

1.5.8. Kundensupport- und Sytemadministrationsnachrichten

[0510] Das DPC verwaltet auch weitere Nachrichtentypen, die als interne Nachrichten klassifiziert sind. Das DPC nimmt im Allgemeinen diese Nachrichten von Nicht-DPC-Systemen nicht an. Die Nachrichten sind Datenbankverkäufer-spezifisch. Doch das interne Netzwerk verwendet DES-verschlüsselte Pakete, um für zusätzliche Sicherheit zu sorgen.

[0511] Die Aufgaben im Bereich Kundensupport und Systemadministration werden mittels der Abfragesprache- und Applikationsentwicklungstools des Datenbankverkäufers implementiert.

1.5.8.1. Kundendienstaufgaben

– IBD: Einträge finden, aktivieren, deaktivieren, entfernen, korrigieren
– AID: autorisierte Individuen hinzufügen oder löschen
– AOD: Einträge finden, hinzufügen, entfernen, korrigieren
– VAD: Einträge finden, aktivieren, deaktivieren, entfernen, korrigieren
– RMD: Einträge finden, hinzufügen, entfernen, korrigieren
– PFD: Einträge hinzufügen, entfernen, korrigieren

1.5.8.2. Systemadministrationsaufgaben

– Durchführung von Vorab-Betrugskontrollen
– Modifizieren der Liste gültiger Standorte
– Zusammenfassen protokollierter Informationen (Warnungen, Fehler usw.)
– Modifizieren der PIC-Gruppen-Liste
– Performance-Monitoring
– Durchführung von Sicherungen
– Verfahren zur Behebung von Systemabstürzen (Crash Recovery)
– Zeitsynchronisierung für die DPC-Standorte
– Wechsel der primären Registrierungsstelle
– Änderung des geheimen DES-Verschlüsselungsschlüssels
– Säuberung alter Dokumentverfolgungsnummern
– Erstellen einer Liste mit BIA-Hardware-Identifizierungscode, MAC-Verschlüsselungsschlüssel und DUKPT-Basisschlüssel-Tripeln; Speichern auf einer verschlüsselten Diskette für das Schlüsselladegerät

1.5.9. Firewall-Vorrichtung

1.5.9.1. Zweck

[0512] Die FW-Vorrichtung bietet eine erste Verteidigungslinie vor Netzviren und Computerhackern. Alle Kommunikationsverbindungen in den oder aus dem DPC-Standort gelangen zuerst durch eine sichere FW-Vorrichtung.

1.5.9.2. Verwendung

[0513] Die FW-Vorrichtung, ein Internet-Localnet-Router, ist nur für Nachrichten zuständig, die für die GM-Vorrichtungen bestimmt sind.

[0514] Mit BIA ausgestattete Endgeräte senden Pakete über ein Modem, X.25 oder ein anderes Kommunikationsmedium an eine einzige DPC-Stelle. Das DPC verlässt sich auf einen Dritten, der die Modembanken bereitstellt, deren Aufgabe darin besteht, die einlangenden Anrufe zu bearbeiten und die Daten in das DPC-Backbone zu füttern.

[0515] Für die DPC-zu-DPC-Kommunikation vor allem für dezentrale Transaktionen und Folgenummeraktualisierungen, versenden die FW-Vorrichtungen DES-entschlüsselte Pakete doppelter Länge. Die DPC-LAN-Komponente ist für Ver- und Entschlüsselung zuständig – die FWs haben die Fähigkeit zur Paketentschlüsselung nämlich nicht.

1.5.9.3. Sicherheit

[0516] Ein richtig konfigurierter Netzwerkschnüffler dient – als Backup für die FW – als Detektor von Eindringlingen. Wenn eine abnormale Nachricht detektiert wird, werden die eindringenden Nachrichten in ihrer Gesamtheit aufgezeichnet, ein Operator wird gewarnt, und die FW wird vom Schnüffler physikalisch geschlossen.

[0517] Die FW erlaubt keine Übertragungen vom internen Netz in den übrigen Teil des Internets.

1.5.9.4. Nachrichtenbandbreite

[0518] Eine Transaktionsautorisierungs-Anfrage erfordert etwa 400 Byte, und Registrierungspakete erfordern etwa 2 kB. Um 1000 Transaktionsautorisierungen pro Sekunde und 1 Registrierungspaket pro Sekunde bewältigen zu können, sind die FW-Vorrichtungen in der Lage, etwa 400 kB pro Sekunde zu verarbeiten (all dies ist auf dem Gebiet der Erfindung bekannt).

[0519] Jede DPC-Stelle erfordert eine gesamte Bandbreite von nahezu drei T1-Verbindungen zur Modembank des Drittteilnehmers und den anderen DPC-Standorten.

1.5.10. Gateway-Vorrichtung

1.5.10.1. Zweck

[0520] Die GM verbindet über die FW-Vorrichtungen die Außenwelt (mit BIA ausgestattete Endgeräte und andere DPCs) mit den internen Komponenten des DPC. Das DPC besitzt mehrere GMs, üblicherweise zwei.

1.5.10.2. Verwendung

[0521] Die GM überwacht die Verarbeitung jeder BIA-Anfrage, kommuniziert mit den diversen DPC-Komponenten und übermittelt die verschlüsselten Ergebnisse der anfragenden Bank an den Absender. Die diese Aufgabe erfüllende Software wird als Nachrichtenverarbeitungsmodul (Message Processing Module) bezeichnet.

[0522] Die GM protokolliert alle von ihr empfangenen Anfragen und Warnungen von Komponenten, mit denen sie kommuniziert. Beispielsweise protokolliert die GM allfällige Notfallskontozugriffe, Folgenummerlücken und ungültige Pakete.

[0523] Die Abwicklung einer Anfrage kann es erforderlich machen, dass die GM die GMs aller anderen DPC-Standorte von einer Änderung in den DPC-Datenbanken informiert. Wenn dies eintritt, startet die GM eine

dezentrale Transaktion, um die Ferndatenbanken zu aktualisieren.

[0524] Es gibt zwei Kategorien von dezentralen Transaktionen: synchrone und asynchrone. Bei synchronen dezentralen Transaktionen muss die GM auf die Bestätigung der dezentralen Transaktion warten, bevor sie mit der Verarbeitung des Pakets fortfahren kann. Bei asynchronen dezentralen Transaktionen muss die GM nicht auf die Bestätigung warten; sie kann die Abwicklung der Anfrage abschließen, ob nun die Bestätigung der dezentralen Transaktion vorliegt oder nicht. Asynchrone dezentrale Transaktionen werden nur dazu verwendet, Daten zu aktualisieren, für die Datenbankkonsistenz keine absolute Notwendigkeit darstellt: Folgenummern und biometrische Prüfsummenaufzeichnungen können asynchron ablaufen, während dies beim Anlegen von Datenbankeinträgen wie z. B. von individuellen biometrischen Einträgen nicht der Fall ist.

[0525] Bei der Ausführung einer synchronen dezentralen Transaktion betrachtet die anfragende GM die gesamte Transaktion nur dann als erfolgreich, wenn alle Stellen die Transaktion lokal erfolgreich bestätigen können. Andernfalls machen die GMs die Veränderungen lokal rückgängig und weisen die Anfrage infolge eines Transaktionsfehlers ab.

[0526] Die Liste gültiger DPC-Stellen umfasst normalerweise alle Standorte. Im Fall eines extremen Standortversagens jedoch kann ein Systemadministrator diese Stelle von der Liste gültiger Stellen streichen. Die wahrscheinlichsten Ursachen für dezentrales Transaktionsversagen sind allerdings vorübergehende Netzausfälle, die mit der DPC-Ausrüstung nicht in Zusammenhang stehen. Anfragen, die eine synchrone dezentrale Transaktion erfordern, können erst dann durchgeführt werden, wenn die Netzwerkkonnektivität wiederhergestellt oder die Stelle von der Liste gültiger Standorte gestrichen ist. Bevor eine Steile wieder auf die Liste gültiger Standorte gesetzt werden kann, gleicht der Systemadministrator die Datenbanken der Stelle mit jenen einer derzeit aktiven Stelle ab.

1.5.10.3. Softwarekomponenten

[0527] Jede GM lässt lokal aus Gründen der Performance die folgenden Softwarekomponenten laufen:
Nachrichtenverarbeitungs-Modul
Nachrichtenautentisierungscode-Modul
Nachrichtenentschlüsselungs-Modul
Liste der individuellen biometrischen Datenbanken

1.5.10.4. Nachrichtenbandbreite

[0528] Die von GMs benötigte Nachrichtenbandbreite ähnelt der von FW-Vorrichtungen benötigten Bandbreite. Eine FDDI-Netzwerkschnittstelle bietet 100 MB pro Sekunde und deckt leicht die Bandbreitenanforderungen ab.

1.5.11. DPC LAN

1.5.11.1. Zweck

[0529] Das DPC Local Area Network (LAN) verbindet die Maschinen der DPC-Stellen mittels eines Lichtwellenleiter-Token-Rings miteinander. Der Lichtwellenleiter-Token-Ring sorgt sowohl für hohe Bandbreite als auch für zufrieden stellende physikalische Sicherheit.

1.5.11.2. Sicherheit

[0530] Die von den Maschinen im DPC LAN verwendeten Netzwerkschnittstellen enthalten Verschlüsselungshardware, um das Abhören oder Abfangen von Paketen ohne den Verschlüsselungsschlüssel sinnlos zu machen. Der Verschlüsselungsschlüssel ist für alle Vorrichtungen im LAN derselbe und wird in der Verschlüsselungshardware gespeichert.

[0531] Ein richtig konfigurierter Netzwerkschnüffler dient – als Backup für die FW – als Detektor von Eindringlingen. Wenn eine abnormale Nachricht detektiert wird, werden die eindringenden Nachrichten in ihrer Gesamtheit aufgezeichnet, ein Operator wird gewarnt, und die FW wird vom Schnüffler physikalisch geschlossen.

1.5.12. Nachrichtenverarbeitungs-Modul

1.5.12.1. Zweck

[0532] Das MPM ist für die Verarbeitung für Anfragepakete zuständig. Es kommuniziert in dem Maße, in dem dies zur Durchführung der Aufgaben notwendig ist, mit anderen Komponenten des DPC. Die Gegenwart eines MPM in einer Maschine macht sie zu einer GM.

1.5.12.2. Nutzung

[0533] Das MPM hält einen Anfragekontext für jede Anfrage, die es aktuell abwickelt, aufrecht. Der Anfragekontext umfasst die Informationen, die notwendig sind, um die Netzwerkverbindung zum die Anfrage stellenden Endgerät beizubehalten, die BIA-Informationen, den Antwortschlüssel und das Antwortpaket.

1.5.13. Nachrichtenautentifizierungscode-Modul

1.5.13.1. Zweck

[0534] Die Aufgaben des MACM bestehen darin, den MAC einlangender Pakete zu validieren und den abgehenden Paketen einen MAC anzufügen.

1.5.13.2. Nutzung

[0535] Das MACM verwaltet eine im Speicher befindliche Hash-Tabelle von 112-bit-MAC-Verschlüsselungsschlüsseln (den Schlüssel bildet der BIA-Hardware-Identifizierungscode).

[0536] Wenn das MACM eine Anfrage von der GM erhält, wonach der MAC eines Pakets zu validieren ist, sieht es zunächst den Hardware-Identifizierungscode des Pakets in der Hash-Tabelle nach. Wenn kein Eintrag besteht, antwortet das MACM der GM mit der Fehlermeldung „ungültiger Hardware-Identifizierungscode".

[0537] Andernfalls nimmt das MACM eine MAC-Kontrolle im BIA-Nachrichtenteil des Pakets mittels des 112-bit-MAC-Verschlüsselungsschlüssels vor. Wenn die MAC-Kontrolle fehlschlägt, antwortet das MACM der GM mit einer „ungültiger MAC"-Fehlermeldung. Wenn nicht, reagiert das MACM mit einer „gültiger MAC"-Nachricht.

[0538] Wenn das Paket einen Händlercode enthält, vergleicht das MACM diesen mit dem Besitzeridentifizierungscode in der Hash-Tabelle. Wenn die Codes nicht übereinstimmen, antwortet das MACM mit einer „ungültiger Besitzer"-Fehlermeldung.

[0539] Wenn das MACM eine Anfrage von der GM erhält, wonach ein MAC für ein Paket zu erstellen ist, sieht es den MAC-Verschlüsselungsschlüssel mittels des Hardware-Identifizierungscodes des Pakets nach. Mit dem MAC-Verschlüsselungsschlüssel erstellt das MACM einen MAC und fügt ihn an das Paket an. Wenn das MACM den Hardware-Identifizierungscode in seiner Hash-Tabelle nicht finden kann, antwortet es stattdessen mit der Fehlermeldung „ungültiger Hardeware-Identifizierungscode".

1.5.13.3. Datenbankschema

[0540] Der MACM-Hash-Tabellen-Eintrag enthält das Folgende:
MACM-Eintrag:
hardwareId = int4
ownerId = int4
macEncryptionKey = int16

[0541] Die Tabelle wird durch den Hardware-Identifizierungscode gehasht.

1.5.13.4. Datenbankgröße

[0542] Unter der Annahme, dass 5 Millionen mit BIA ausgestattete Geräte im Einsatz stehen, erfordert die Hash-Tabelle etwa 120 MB Speicher. Aus Gründen der Performance wird diese Hash-Tabelle komplett im Speicher gecached.

1.5.13.5. Abhängigkeiten

[0543] Das MACM enthält nur Einträge zu aktiven BIA-Hardware-Identifizierungscodes und aktiven Besitzern von Vorrichtungen. Wenn eine Vorrichtung oder ein Besitzer einer Vorrichtung suspendiert oder aus dem System gelöscht wird, entfernt das MACM alle Einträge, die auf den Identifizierungscode Bezug haben. Wenn eine Vorrichtung aktiviert wird, fügt das MACM einen Eintrag dafür an.

[0544] Das MACM cacht den MAC-Verschlüsselungsschlüssel auch aus der VAD. Da das System keinen Wechsel eines Verschlüsselungsschlüssels einer BIA erlaubt, muss sich das MACM keine Sorgen bezüglich des Empfangs von Updates von Verschlüsselungsschlüsseln machen.

1.5.14. Nachrichtenentschlüsselungs-Modul

1.5.14.1. Zweck

[0545] Die Aufgabe des MDM besteht darin, den DUKPT-Transaktionsschlüssel zu rekonstruieren und ihn mit dem Biometrik-PIC-Block des Pakets zu entschlüsseln. Es verwaltet eine Liste von DUKPT-Basisschlüsseln, die zur Erzeugung des Transaktionsschlüssels notwendig sind.

1.5.14.2. Nutzung

[0546] Das MDM konstruiert den DUKPT-Transaktionsschlüssel unter Verwendung der Folgenummer des Pakets als DUKPT-Transaktionszähler, die höheren 22 Bits des BIA-Hardware-Identifizierungscodes als DUKPT-originalgesicherte Sicherheitsmodul-(„TRSM"-) Identifizierung und die 10 niedrigen Bits des BIA-Hardware-Identifizierungscodes als DUKPT-Schlüsselsatzidentifizierung.

[0547] Der DUKPT-Standard spezifiziert, wie der Transaktionsschlüssel generiert wird. Die Schlüsselsatzidentifizierung dient dazu, einen Basisschlüssel in der Liste von Basisschlüsseln nachzusehen. Der Basisschlüssel dient zu, die TRSM-Identifizierung in den Anfangsschlüssel umzuwandeln; dies erfolgt über einen DES-Verschlüsselungs/Entschlüsselungs/Verschlüsselungs-Zyklus. Der Transaktionszähler wird dann an den Anfangsschlüssel als Reihe von DES-Verschlüsselungs/Entschlüsselungs/Verschlüsselungs-Zyklen angelegt, um den Transaktionsschlüssel zu bilden.

[0548] Um die Sicherheit zu erhöhen, bestehen zwei Listen mit Basisschlüsseln – eine für BIAs geringer Sicherheitsstufe und eine für Hochsicherheits-Vorrichtungen. Das MDM wählt je nach Sicherheitsstufe der Vorrichtung aus, welche Basisschlüsselliste zu verwenden ist.

1.5.14.3. Datenbankschema

[0549] Der MDM-Basisschlüssellisten-Eintrag enthält das Folgende:
MDM-Eintrag:
baseKey = int16

[0550] Die Liste mit Basisschlüsseln ist durch Schlüsselsatzidentifizierung indexiert.

1.5.14.4. Datenbankgröße

[0551] Das MDM verwaltet eine im Speicher befindliche Liste von DUKPT-Basisschlüsseln. Jeder Schlüssel benötigt 112 Bits. Das MDM besitzt zwei Sätze von 1024 Schlüsseln, die insgesamt 32 KB benötigen.

1.5.14.5. Abhängigkeiten

[0552] Das MDM ist in keiner Weise direkt von anderen DPC-Komponenten abhängig.

1.5.15. PIC-Gruppen-Liste

1.5.15.1. Zweck

[0553] Die PGL definiert in Verbindung mit der IBD-Maschinen-Liste die Konfiguration der IBD-Maschinen. Die PGL speichert eine Liste der PIC-Gruppen im System, die zur Vereinfachung der PIC-Verwaltung dient.

Eine PIC-Gruppe ist ein Satz aufeinander folgender PIC-Codes. Es existiert eine PGL für jede GM.

1.5.15.2. Nutzung

[0554] Die PGL durchsucht – wenn sie einen PIC-Code erhält – ihre Liste an PIC-Gruppen nach der den PIC-Code enthaltenden Gruppe. Die PGL hält die Gruppen-Liste in einer Reihenfolge und wendet binäre Suche an, um die korrekte Gruppe rasch zu finden.

[0555] Die Anfangskonfiguration für die PGL ist eine riesige PIC-Gruppe, die alle möglichen PICs enthält. Nach der Zuweisung einer Schwellenzahl von PICs wird die PIC-Riesengruppe zweigeteilt. Danach wird dieses Verfahren auf alle nachfolgenden PIC-Gruppen angewendet.

[0556] Wenn eine PIC-Gruppe geteilt wird, weist die PGL eine neue Haupt- und Sicherungs-IBD-Vorrichtung zu; dies erfolgt auf der Basis verfügbarer Speichermenge und nach dem „Wer zuerst kommt, mahlt zuerst"-Prinzip. Die PGL koordiniert sich mit den IBD-Vorrichtungen, um zunächst die betroffenen Einträge aus den alten Haupt- und Sicherungsmaschinen auf die neuen zu kopieren, aktualisiert den IML-Eintrag und entfernt schließlich die alten Haupt- und Sicherungskopien. Das Teilen einer PIC-Gruppe ist eine aufwendige Angelegenheit. Die PGL-Stapel teilen Anfragen, die dann abgearbeitet werden können, wenn das DPC wenig belastet ist, z. B. am Abend bzw. in der Nacht.

[0557] Der Systemadministrator kann auch die Haupt- und Sicherungs-IBD-Maschinen für eine bestimmte PIC-Gruppe ändern, wenn die freie Speichermenge der Maschinen unter einen Wert fällt, der zur Bewältigung des erwarteten Volumens neuer Registrierungen notwendig ist.

1.5.15.3. Datenbankschema

[0558] Das Schema für die PIC-Gruppen-Einträge ist folgendermaßen aufgebaut:
PICGroup: (PIC-Gruppe)
lowPin = int8
highPin = int8
used = int4

[0559] Jede PIC-Gruppe ist durch ein eindeutiges Kennzeichen identifiziert. Aus praktischen Gründen ist der PIC-Gruppen-Identifizierungscode der lowPin-Code für die Gruppe, doch das System ist sonst nicht davon abhängig.

[0560] Die PGL wird durch das lowPin-Feld eingegeben.

1.5.15.4. Datenbankgröße

[0561] Man kann erwarten, dass die PGL etwa 3.000 Gruppen enthält (jede PIC-Gruppe enthält etwa 1.000 aktive PICs, kann aber auch Millionen tatsächlicher PICs enthalten). Die gesamte PGL erfordert etwa 72 KB Speicher und wird komplett im Speicher gecached.

1.5.15.5. Abhängigkeiten

[0562] Wenn PIC-Gruppen hinzugefügt, zusammengefügt oder geteilt werden, ist die PGL dafür verantwortlich, die IBD-Vorrichtungs (Machine)-Liste über Änderungen zu informieren und die Bewegung von IBD-Einträgen von einer IBD-Vorrichtung (Machine) zur anderen zu steuern.

1.5.16. Individuelle Biometrische Datenbank (IBD)-Liste

1.5.16.1. Zweck

[0563] Die IBD-Vorrichtungs-Liste (IML) codiert gemeinsam mit der PIC-Gruppen-Liste die Konfiguration der IBD-Vorrichtungen. Die IML bildet einen PIC-Code in die Haupt- und Sicherungs-IBD-Vorrichtungen ab, die IBD-Einträge für den PIC speichern. Den Schlüssel für die IML bildet die PIC-Gruppe (ein Satz aufeinander folgender PIC-Codes) und nicht individuelle PICs, da dies die zum Speichern der Liste erforderliche Speichermenge stark reduziert. Es gibt in jeder GM eine IML.

1.5.16.2. Nutzung

[0564] Wenn eine GM eine Anfrage abwickelt, die eine biometrische Identifizierung erfordert, findet die GM den IML-Eintrag, dessen Schlüssel die Biometrik-PIC-Gruppe ist. Die GM kennt dann die für die biometrische Identifizierung zu verwendenden Haupt- und Sicherungs-IBD-Vorrichtungen.

1.5.16.3. Datenbankschema

[0565] Das Schema für die Einträge der IML-Liste ist folgendermaßen aufgebaut:
MachinePair:
pinGroup = int8
main = int2
backup = int2

[0566] Der Schlüssel für die IML ist die pinGroup.

1.5.16.4. Datenbankgröße

[0567] Man kann davon ausgehen, dass die IML etwa 3.000 Einträge (die Anzahl an PIC-Gruppen) enthält. Jeder MachinePair-Eintrag besteht aus 12 Bytes, die etwa 36 kB Speicher erfordern, und wird komplett im Speicher gecached.

1.5.16.5. Abhängigkeiten

[0568] Allfällige Änderungen hinsichtlich der Konfiguration der IBD-Vorrichtungen spiegeln sich in der IML wider. Außerdem verwendet die IML PIC-Gruppen für ihre Schlüssel, so dass beim Modifizieren der PIC-Gruppen-Liste auch die IMLs aktualisiert werden.

1.5.17. Folgenummermodul

1.5.7.1. Zweck

[0569] Die primäre Funktion des SNM liegt darin, Wiedergabeangriffe zu verhindern, indem Paketfolgenummern validiert werden. Die zweite Aufgabe ist es, die Auswirkungen eines auf Wiedervorlage basierenden Angriffs zu minimieren, indem andere SNMs an entfernten DPC-Stellen von Folgenummerupdates informiert und die Folgenummern in der VAD regelmäßig aktualisiert werden.

[0570] Das SNM verwaltet eine im Speicher befindliche Hash-Tabelle von Folgenummern (den Schlüssel bildet der BIA-Hardware-Identifizierungscode), um eine rasche Validierung von Folgenummerpaketen zu ermöglichen.

1.5.17.2. Benutzung

[0571] Wenn das SNM eine Validierungsanfrage von der GM für einen bestimmten Hardware-Identifizierungscode und eine bestimmte Folgenummer erhält, sieht es den Hardware-Identifizierungscode in der Hash-Tabelle nach. Wenn kein Eintrag besteht, antwortet das SNM der GM mit einer „ungültiger Hardware-Identifizierungscode"-Fehlermeldung.

[0572] Andernfalls überprüft das SNM die bestimmte Folgenummer und vergleicht sie mit der im Hash-Tabellen-Eintrag gespeicherten Folgenummer. Wenn die Folgenummer kleiner als die gespeicherte Folgenummer ist oder ihr entspricht, antwortet das SNM mit einer Fehlermeldung lautend auf „ungültige Folgenummer". Wenn nicht, setzt das SNM die Folgenummer im Hash-Tabellen-Eintrag auf die bestimmte Folgenummer und antwortet mit einer auf „gültige Folgenummer" lautenden Nachricht.

[0573] Manchmal kann das SNM eine Folgenummerlücke beobachten. Eine Folgenummerlücke tritt auf, wenn ein SNM eine Folgenummer empfängt, die um mehr als 1 höher ist als die im Hash-Tabellen-Eintrag gespeicherte Folgenummer. Anders ausgedrückt wurde eine Folgenummer übersprungen. Wenn das SNM eine Folgenummerlücke entdeckt, reagiert es mit der an die GM gesendeten Nachricht „Folgenummerlücke" und nicht mit der Nachricht „gültige Folgenummer". Die GM betrachtet das Paket als gültig, protokolliert aber eine auf „Folgenummerlücke" lautende Warnung.

[0574] Folgenummerlücken treten üblicherweise auf, wenn die Netzwerkkonnektivität gesunken ist: Pakete werden fallen gelassen oder können erst dann zugestellt werden, wenn die Netzfunktion wiederhergestellt ist. Folgenummerlücken treten jedoch auch aufgrund betrügerischer Handlungen auf: böswillige Personen könnten Pakete abfangen, wodurch sie nicht im DPC eintreffen, oder sie könnten sogar versuchen Pakete zu fälschen (mit einer hohen Folgenummer, so dass das Paket nicht sofort abgewiesen wird).

[0575] Die zweite Funktion des SNM besteht darin, andere DPCs über die aktualisierten Folgenummern zu informieren. Das rasche Updaten von Folgenummern an allen DPC-Standorten vereitelt auf Wiedervorlage basierende Angriffe, bei denen ein böswilliger Teilnehmer Pakete beobachtet, deren Ziel eine DPC-Stelle ist, und sofort eine Kopie an einen anderen DPC-Standort schickt – in der Hoffnung, die Übertragungsverzögerung der Folgenummerupdates von einer DPC-Stelle zur anderen auszunützen, was dazu führt, dass beide Standorte das Paket als gültig annehmen, während aber nur der erste Standort das Paket annehmen sollte.

[0576] Die SNMs schicken einander Aktualisierungsnachrichten, wenn sie eine gültige Folgenummer erhalten. Wenn ein SNM eine Aktualisierungsmeldung für eine Folgenummer erhält, die kleiner als die aktuell in seiner Hash-Tabelle gespeicherte Folgenummer ist oder ihr entspricht, protokolliert das SNM eine Folgenummer-Wiedervorlagewarnung. Alle auf Wiedervorlage basierenden Angriffe werden auf diese Weise detektiert.

[0577] Eine einfachere Möglichkeit, diese auf Wiedervorlage basierenden Angriffe vollkommen zu vereiteln, besteht darin, nur ein SNM vorzusehen, das Pakete validiert. Gemäß diesem Schema gibt es keine Möglichkeit, die Übertragungsverzögerung beim Update mittels eines auf Wiedervorlage basierenden Angriffs auszunutzen. Alternativ dazu können mehrere SNMs gleichzeitig aktiv sein, sofern keines von ihnen die Folgenummervalidierung für dieselbe mit BIA ausgestattete Vorrichtung durchführt.

1.5.17.3. Folgenummerwartung

[0578] Wenn ein SNM hochfährt, lädt es die Folgenummer-Hash-Tabelle aus den Folgenummern für aktive im VAD gespeicherte BIAs.

[0579] Einmal pro Tag lädt das SNM die aktuellen Folgenummern für die lokale VAD herunter.

[0580] Die VAD ist für das Versenden von „Eintrag hinzufügen"- und „Eintrag entfernen"-Meldungen an die SNM für alle mit BIA ausgestatteten Vorrichtungen verantwortlich, die aktiviert oder deaktiviert sind, damit die SNM-Hash-Tabelle immer aktualisiert ist.

1.5.17.4. Datenbankschema

[0581] Der SNM-Hash-Tabellen-Eintrag enthält das Folgende:
SNM-Eintrag:
hardwareId = int4
sequenceNumber = int4

[0582] Den Schlüssel für die Hash-Tabelle bildet hardwareId.

1.5.17.5. Datenbankgröße

[0583] Unter der Annahme von etwa 5 Millionen im Einsatz stehender BIA-Vorrichtungen erfordert die Hash-Tabelle etwa 40 MB.

1.5.17.6. Abhängigkeiten

[0584] Das SNM hängt von der VAD ab. Wenn eine Vorrichtung suspendiert oder aus der Datenbank entfernt ist, löscht das SNM den entsprechenden Eintrag. Wenn eine Vorrichtung aktiviert ist, legt das SNM dafür einen Eintrag an.

1.5.17.7. Nachrichtenbandbreite

[0585] Die SNMs erfordern eine Übertragungsbandbreite von etwa 8 KB pro Sekunde, um 1.000 Update-Folgenummernachrichten pro Sekunde zu bewältigen. Die Update-Folgenummernachrichten werden gepuffert und einmal pro Sekunde verschickt, um die Anzahl der tatsächlich gesendeten Nachrichten zu minimieren.

1.5.18. Gerätebesitzer-Datenbank (AOD)

1.5.18.1. Zweck

[0586] Die AOD speichert Informationen über Individuen oder Organisationen, die eine oder mehrere mit BIA ausgestattete Geräte besitzen. Diese Information dient dazu, genau zu kontrollieren, ob die BIAs nur von ihren rechtmäßigen Besitzern verwendet werden, um Kontoinformationen für Gutschrift- und Lastschrift-Finanztransaktionen zu liefern, und ermöglicht die Identifizierung aller BIAs, die im Besitz eines bestimmten Individuums oder einer bestimmten Organisation stehen.

1.5.18.2. Nutzung

[0587] Jeder AOD-Eintrag enthält ein Finanzkonto, um für den Besitzer eine Gut- oder Lastschrift zu verbuchen, wenn das DPC eine Finanztransaktion abwickelt, die von einer der mit BIA ausgestatteten Vorrichtungen des Besitzers vorgelegt wird. Beispielsweise umfassen Transaktionen, die von einer an ein RPT angeschlossenen BIA initiiert werden, Kontogutschriften, während zertifizierte E-Mail-Übertragungen zu Kontolastschriften führen.

1.5.18.3. Datenbankschema

[0588] Das Schema für den den Gerätebesitzer betreffenden Eintrag ist folgendermaßen:
ApparatusOwner (Gerätebesitzer)
ownerID = int4
name = char50
address = char50
zipCode = char9
assetAccount = char16
status = int1

[0589] Das Statusfeld ist entweder:
0: suspendiert oder
1: aktiv

[0590] Den Schlüssel für die AOD bildet ownerId.

1.5.18.4. Datenbankgröße

[0591] Man kann davon ausgehen, dass die AOD etwa 2 Millionen Gerätebesitzer-Einträge speichert. Jeder Eintrag umfasst 130 Byte und erfordert etwa 260 MB Speicher. Die AOD wird als gehashte Datei gespeichert (den Schlüssel bildet der nach Besitzer-Identifizierungscode). Eine Kopie der AOD ist in jeder GM gespeichert.

1.5.18.5. Abhängigkeiten

[0592] Wenn Einträge aus der AOD entfernt oder suspendiert werden, werden alle VAD-Einträge mit einer Bezugnahme auf diese Gerätebesitzer als suspendiert vermerkt. Außerdem löschen das MAC-Modul und das Folgenummermodul ihre Einträge für die suspendierten Vorrichtungen.

1.5.19. Datenbank betreffend die Validität des Gerät (VAD)

1.5.19.1. Zweck

[0593] Die VAD ist eine Sammlung von Einträgen, die alle bislang hergestellten BIAs darstellen. Der VAD-Eintrag enthält auch den MAC-Verschlüsselungsschlüssel für jede BIA sowie die Angabe, ob eine BIA aktiv ist, zugestellt werden soll oder als zerstört markiert ist. Damit eine Nachricht von der BIA entschlüsselt werden kann, muss die BIA existieren und einen aktiven Eintrag in der VAD aufweisen.

1.5.19.2. Nutzung

[0594] Bei der Herstellung besitzt jede BIA einen eindeutigen öffentlichen Identifizierungscode und einen eindeutigen MAC-Verschlüsselungsschlüssel, von denen beide vor dem BIA-Einsatz im VAD-Eintrag vermerkt

werden.

[0595] Wenn eine BIA zunächst gebildet wird, erhält sie einen eindeutigen Hardware-Identifizierungscode. Wenn eine BIA in Betrieb genommen wird, wird ihr Hardware-Identifizierungscode im System registriert. Zunächst wird der Besitzer oder der Verantwortliche der BIA in die AOD eingetragen. Dann wird der VAD-Eintrag dem AOD-Eintrag zugewiesen und die BIA in Betrieb genommen. Anfragen seitens der BIA werden vom DPC angenommen.

[0596] Wenn eine BIA aus dem Verkehr gezogen wird, wird sie als inaktiv markiert, und die Verbindung zum AOD-Eintrag wird abgebrochen. Es werden keine Kommunikationen mehr von dieser BIA angenommen.

[0597] Jeder BIA-Typ und jedes BIA-Modell besitzt eine ihm zugeteilte Sicherheitsstufe, die das tatsächliche Sicherheitsniveau angibt. Wenn das DPC Anfragen von dieser BIA bearbeitet, wendet es die Sicherheitsstufe der BIA an, um zu ermitteln, welche Handlungen erlaubt sind. Das DPC bietet diese Sicherheitsstufe auch für externe Finanztransaktions-Autorisierungsdienste an.

[0598] Beispielsweise kann sich ein Finanztransaktions-Autorisierungsdienst weigern, eine Anfrage für über $ 300 von einer BIA mit niedriger Sicherheitsstufe zu bearbeiten; in diesem Fall müssten Personen BIAs höherer Sicherheit verwenden, um solche Gedbeträge zu genehmigen. Der Autorisierungsdienst kann die Sicherheitsstufe auch als Richtschnur heranziehen, wie viel unter Berücksichtigung des Risikos für die Transaktion zu verrechnen ist.

[0599] Die Sicherheitsstufen und die laut ihnen erlaubten Handlungen werden im praktischen Betrieb festgelegt. Die Kosten, die beim Systemmissbrauch entstehen, müssen höher sein als der potenzielle Nutzen – die Sicherheitsstufe steht also mit den Kosten in Zusammenhang, die beim Manipulieren der Vorrichtung auflaufen.

1.5.19.3. Datenbankschema

[0600] Nachstehend das Schema für die Einträge betreffend die Gültigkeit des Geräts:
ValidApparatus: (Gültiges Gerät)
hardwareId = int4
macEncryptionKey = int16
ownerId = int8
mfgDate = time
inServiceDate = time
securityLevel = int2
status = int1
type = int1
use = int1

[0601] Mögliche Werte für das Statusfeld:
0: suspendiert
1: aktiv
2: zerstört

[0602] Mögliche Werte für das Typenfeld (einer für jeden Endgerätetyp):
0: ATM
1: BRT
2: CET
3: CPT
4: CST
5: EST
6: IPT
7: IT
8: ITT
9: PPT
10: RPT
11: SFT

[0603] Mögliche Werte für das Benutzungsfeld:
0: Einzelhandel
1: persönlich
2: Aussteller
3: fern

[0604] Der Schlüssel für die VAD ist der Hardware-Identifizierungscode.

1.5.19.4. Datenbankgröße

[0605] Die VAD bearbeitet etwa 5 Millionen Einzelhandels-, Aussteller- und Fern-Einträge betreffend die Gültigkeit des Geräts. Jeder Eintrag umfasst 51 Bytes und erfordert insgesamt etwa 255 MB. Die VAD ist als gehashte Datei gespeichert, deren Schlüssel der Hardware-Identifizierungscode ist. Eine Kopie der VAD ist in jeder GM gespeichert.

[0606] Die Anzahl persönlicher Einträge betreffend die Gültigkeit des Geräts liegt im Bereich von 30 Millionen, was eine Speicherkapazität von zusätzlich 1,5 GB erfordert.

1.5.19.5. Abhängigkeiten

[0607] Wenn ein VAD-Eintrag seinen Status ändert, werden die MAC-Module und die SNMs von dieser Statusänderung informiert. Wenn z. B. ein Gerät aktiv wird, fügen das MACP und das SNM einen Eintrag für das neue aktive Gerät an. Wenn ein Gerät inaktiv wird, löschen das MACP und das SNM ihre Eintragung für dieses Gerät.

1.5.20. Individuelle biometrische Datenbank (IBD)

1.5.20.1. Zweck

[0608] Die IBD-Einträge speichern Informationen über Individuen, d. h. ihre primären und sekundären biometrischen Eingaben, den PIC, die Liste von Finanzkonten, den privaten Code, das Notfallskonto, die Adresse und die private Telefonnummer. Das individuum kann gegebenenfalls auch ihre SSN und ihre E-Mail-Adresse angeben. Diese Informationen sind notwendig, um ein Individuum entweder anhand biometrischer oder persönlicher Informationen zu identifizieren, auf Kontoinformationen zugreifen zu können oder an einem entfernten Ort befindlichen Händlern zwecks zusätzlicher Verifizierung Adresse und Telefonnummer zukommen zu lassen.

1.5.20.2. Nutzung

[0609] Individuen werden während des individuellen Anmeldevorgangs in registrierten biometrischen Registrierungsendgeräten, die sich weltweit in Bankfilialen oder in lokalen Büros befinden, in das System eingetragen. Während der Anmeldung wählen Individuen ihre persönlichen Identifizierungsnummern aus und fügen ihre Finanzkonten an ihre Biometrik-PIC-Kombination an.

[0610] Individuen können infolge Betrugs, den ein ausstellendes Mitglied meldet, aus der Datenbank gelöscht werden. Wenn dies eintritt, werden die Kontoinformationen des Individuums durch einen autorisierten internen Systemrepräsentanten von der IBD in die PFD übertragen. Die biometrischen Identifizierungen für Einträge in der PFD können für Einträge in der IBD nicht verwendet werden.

[0611] Der IBD existiert auf mehreren Vorrichtungen, von denen jede für einen Untersatz der IBD-Einträge verantwortlich ist, mit einer Kopie von jedem gespeicherten Eintrag auf zwei verschiedenen Vorrichtungen, beide für Redundanz und Lastaufteilung. Die IBD-Vorrichtungsliste, die auf GM gespeichert ist, verwaltet alle Vorrichtungen und ihre PICs.

1.5.20.3. Datenbankschema

[0612] Nachstehend das Schema für den individuellen biometrischen Eintrag:
IndividualBiometric: (individueller biometrischer Eintrag)
primaryBiometric = biometric
secondaryBiometric = biometric

biometricId = int4
PIC = char10
phoneNumber = char12
lastName = char24
firstName = char24
middleinitial = char2
SSN = char9
privateCode = char40
address = char50
zipCode = char9
publicKey = char64
checksums = int4[10]
accountLinks = char30 [10]
emergencyIndex = char1
emergencyLink = char1
privs = char10
enroller = int8
emergencyUseCount = int4
status = int1

[0613] Das Statusfeld kann folgendermaßen aussehen:
0: suspendiert
1: aktiv
2: früherer Betrug

[0614] Den Schlüssel für die IBD bildet der PIC.

1.5.20.4. Datenbankindizes

[0615] Jede IBD-Vorrichtung verfügt in Bezug auf das Folgende über zusätzliche Indizes, um den Zugriff auf die IBD-Datenbank zu vereinfachen: SSN (Sozialversicherungsnummer), biometrischer Identifizierungscode, Familienname, Vorname und Telefonnummer.

1.5.20.5. Datenbankgröße

[0616] Jede IBD-Maschine besitzt 40 GB Sekundärspeicher (bereitgestellt durch eine oder mehrere RAID-Geräte). Jeder IBD-Eintrag ist 2658 Bytes groß (unter der Annahme, dass die biometrische Eingabe jeweils 1 K groß ist), so dass bis zu 15 Millionen Einträge pro Maschine möglich sind. Die IBD-Einträge werden unter Verwendung eines – möglicherweise geclusterten – Sekundärindex im PIC gespeichert. Der Index wird im Speicher gespeichert und erfordert höchsten 64 MB (ein 64 MB-Index bewältigt etwa 16 Millionen Einträge). Um Einträge für 300 Millionen Individuen zu speichern, benötigt das DPC zumindest 40 IBD-Maschinen: 20 IBD-Maschinen für die Hauptspeicherung und weitere 20 für die Sicherung. Die Anzahl der IBD-Maschinen kann je nach Anzahl registrierter Individuen problemlos erhöht oder verringert werden.

1.5.20.6. Abhängigkeiten

[0617] Die IBD-Maschinen, die PIC-Gruppen-Liste und die IBD-Maschinen-Liste werden in Bezug auf Informationen, welche PICs für welche Maschinen gelten, immer aktualisiert. Wenn eine PIC-Gruppe rekonfiguriert wird oder wenn Haupt- und Sicherungsmaschinen für PIC-Gruppen geändert werden, aktualisieren die IBD-Maschinene ihre Datenbanken und Indizes dementsprechend.

1.5.21. Datenbank über autorisierte Individuen

1.5.21.1. Zweck

[0618] Für jeden Aussteller oder jedes mit persönlicher BIA ausgestattetes Gerät verwaltet die AID eine Liste von Individuen, die durch den Gerätebesitzer ermächtigt wurden, sie zu benutzen.

[0619] Die AID besteht aus zwei Gründen. Der erste besteht darin, dass sie beschränkten Zugang zu einem Endgerät bietet. Beispielsweise kann das Ausstellerendgerät nur von einem autorisierten Bankmitarbeiter ver-

wendet werden. Der zweite Grund besteht darin, Kriminelle daran zu hindern, geheim die BIA in einem RPT durch jene einer persönlichen BIA aus einem Telefonendgerät zu ersetzen, wodurch sie alle Einkäufe auf ein von den Kriminellen eröffnetes Fernhändlerkonto abzweigen können.

1.5.21.2. Datenbankschema

[0620] Das Schema für den Eintrag betreffend autorisierte Individuen sieht folgendermaßen aus:
AuthorizedIndividual (autorisiertes Individuum)
hardwareId = int4
biometricId = int4

[0621] Der hardwareId bezieht sich auf einen Eintrag in der VAD, und der biometricId bezieht sich auf einen Eintrag in der IBD. Wenn das DPC überprüfen muss, ob ein Individuum autorisiert ist, eine persönliche oder Aussteller-BA zu verwenden, kontrolliert es, ob ein Eintrag betreffend autorisierte Individuen mit dem korrekten hardwareId und biometricId besteht.

[0622] Persönliche BIAs werden durch ein auf 1 (persönlich) gesetztes Nutzungsfeld in der VAD identifiziert. Aussteller-BIAs werden durch ein auf 2 (Aussteller) in der VAD gesetztes Nutzungsfeld identifiziert.

1.5.21.3. Datenbankgröße

[0623] Unter der Annahme, dass jedes Ausstellerendgerät von 10 autorisierten Individuen benutzt werden kann und dass jedes persönliche Gerät von 2 zusätzlichen autorisierten Individuen benutzt werden kann, speichert die AID (bei 1.000.000 persönlichen Geräten im Server) etwa die folgende Menge:

10*100.000 + 2*1.000.000 = 3.000.000 Einträge

[0624] Die gesamte Datenbank erfordert etwa 24 MB Speicher.

1.5.21.4. Abhängigkeiten

[0625] Wenn die AOD-Einträge oder VAD-Einträge entfernt werden, werden auch alle auf sie Bezug nehmenden Einträge betreffend autorisierte Individuen entfernt.

1.5.22. Datenbanken über vorherigen Betrug

1.5.22.1. Zweck

[0626] Die PFD ist eine Sammlung von Einträgen über Individuen, die Aussteller in der Vergangenheit betrogen haben. Die PFD lässt auch Hintergrundtransaktionen während Phasen geringer Systemaktivität ablaufen, um Individuen in der IBD herauszufiltern, die übereinstimmende Aufzeichnungen in der PFD aufweisen.

[0627] Das System setzt Individuen nur dann automatisch in die PFD, wenn es detektiert, dass sie eine erneute Registrierung versuchen. Ein Individuum in die PFD zu setzen, ist eine heikle Maßnahme von großer Tragweite, die außerhalb des Bereichs der Erfindung liegt.

1.5.22.2. Nutzung

[0628] Bevor ein neuer IBD-Eintrag als aktiv vermerkt wird, werden die primäre und die sekundäre biometrische Eingabe des Individuums mit jeder biometrischen Eingabe in der PFD verglichen; dabei kommen die gleichen biometrischen Vergleichstechniken zur Anwendung, wie sie in der individuellen Identifizierungsprozedur zum Einsatz kommen. Wenn eine Übereinstimmung für den neuen IBD-Eintrag vorliegt, wird der Status des IBD-Eintrags auf „früherer Missbrauch" gesetzt. Wenn die Überprüfung auf früheren Missbrauch als Teil einer Registrierungsanfrage durchgeführt wurde, protokolliert die GM eine auf „registrierendes Individuum mit früherem Systemmissbrauch" lautende Warnung.

[0629] Man nimmt an, dass die PFD relativ klein bleiben wird. Die Betriebskosten der PFD sind hoch, da es sich um eine unfreiwillige biometrische Suche handelt, und darum ist es wichtig, nur jene Individuen in die PFD zu setzen, die dem System beträchtliche Kosten verursacht haben.

1.5.22.3. Datenbankschema

[0630] Das Schema des Eintrags betreffend früheren Missbrauch sieht folgendermaßen aus:
PriorFraud: (früherer Missbrauch)
primaryBiometric = biometric
secondaryBiometric = biometric
biometricId = int4
PIC = char10
phoneNumber = char12
lastName = char24
firstName = char24
middleInitial = char2
SSN = char9
privateSignal = char40
address = char50
zipCode = char9
publicKey = char64
checksums = int4[10]
accountLinks = char30 [10]
emergencyIndex = char1
emergencyLink = char1
privs = char10
enroller = int8
emergencyUseCount = int4
status = int1

[0631] Das Statusfeld kann folgendermaßen aussehen:
0: suspendiert
1: aktiv
2: früherer Betrug

[0632] Den Schlüssel für die PFD bildet der biometrische Identifizierungscode.

1.5.22.4. Datenbankgröße

[0633] Der PFD-Eintrag ist der gleiche wie der IBD-Eintrag. Glücklicherweise muss das DPC viel weniger davon speichern, so dass nur zwei Datenbankvorrichtungen notwendig sind, um die gesamte Datenbank zu speichern, von denen eine die Sicherung ist.

1.5.22.5. Abhängigkeiten

[0634] Die PFD ist in keiner Weise direkt von anderen DPC-Komponenten abhängig.

1.5.23. Ausstellerdatenbank

1.5.23.1. Zweck

[0635] Die Ausstellerdatenbank (ID) speichert Informationen über Banken und andere Finanzinstitutionen, die ihren Kontozugriff über das System ermöglichen. Die ausstellenden Institutionen sind die einzigen Teilnehmer, die ihre Kontonummern einem bestimmten IBD-Eintrag eines Individuums hinzufügen oder daraus löschen können.

1.5.23.2. Nutzung

[0636] Das DPC bedient sich der ID, um Anfragen von Ausstellerendgeräten zu validieren, indem die ID auf einen Eintrag untersucht wird, der den Ausstellercode des Ausstellerendgeräts enthält. Die im Eintrag gespeicherte Besitzeridentifizierung muss mit dem Besitzer übereinstimmen, der in der VAD für die im Ausstellerendgerät gespeicherte BIA gespeichert ist.

[0637] Das Schema für den Ausstellereintrag sieht folgendermaßen aus:

IssuerRecord: (Ausstellereintrag)
issuerCode = int6
ownerId = int4
name = char50
phoneNumber = char12
address = char50
zipCode = char9

[0638] Den Schlüssel für die Ausstellerdatenbank bildet der Ausstellercode.

1.5.23.3. Datenbankgröße

[0639] Die Ausstellerdatenbank beinhaltet etwa 100.000 Einträge. Jeder Eintrag ist 127 Bytes groß, die weniger als 2 MB erfordern. Eine Kopie der ID ist in jeder GM gespeichert.

1.5.23.4. Abhängigkeiten

[0640] Die Ausstellerdatenbank ist in keiner Weise direkt von irgendwelchen anderen DPC-Komponenten abhängig.

1.5.24. Datenbank für elektronische Dokumente (EDD)

1.5.24.1. Zweck

[0641] Die EDD speichert und verfolgt elektronische Dokumente wie z. B. Faxbilder und E-Mail-Nachrichten für bestimmte Individuen. Sie wartet auch Firmenorganigramme, um die offiziellen Titel von Absendern und Empfängern bereitzustellen. Die EDD archiviert die Dokumente auf Aufforderung des Absenders oder Empfängers und sorgt für Verifizierung der über das System vorgelegten Verträge bzw. Vereinbarungen durch einen neutralen Dritten.

1.5.24.2. Nutzung

[0642] Wenn das DPC ein Fax oder ein anderes elektronisches Dokument von einem Individuum erhält, legt es einen EDD-Dokumenteneintrag an, um das Dokument zu speichern, bis es von den autorisierten Empfängern abgeholt wird.

[0643] Bei Faxdokumenten sind die Empfänger durch Faxnummer und -durchwahl angeführt. Bei anderen elektronischen Dokumenten sind die Empfänger durch E-Mail-Adresse angeführt. Das DPC durchsucht einen Organisationseintrag für jeden Empfänger nach Faxnummer und -durchwahl oder E-Mail-Adresse. Wenn der Eintrag nicht auffindbar ist, sieht das DPC in der IBD nach – aber nur wenn der Empfänger durch E-Mail-Adresse angegeben ist. Für jeden Empfänger legt das DPC einen Empfängereintrag an, der sowohl auf das Dokument als auch auf die biometrische Identifizierung des Empfängers (angegeben von der Organisation oder dem IBD-Eintrag, falls dieser gefunden wird) Bezug nimmt. Das DPC erlaubt im System nicht-registrierte Empfänger, aber es kann keine Zustellung oder Vertraulichkeit für diese Empfänger gewährleistet werden.

[0644] Die EDD ist flexibel genug, um die Übertragung von Faxdokumenten an die E-Mail-Adresse eines Individuums oder die Zustellung von E-Mail-Nachrichten an ein Faxgerät zu ermöglichen.

[0645] Zwar setzt das System keine elektronische Signatur auf das Dokument, doch garantiert es mittels Verschlüsselung, dass die Nachricht, so wie sie durch das Endgerät für zertifizierte E-Mails oder sichere Faxe erhalten (und entschlüsselt) wurde, durch das Individuum gesendet wurde.

[0646] Entsprechend autorisierte Mitarbeiter der Organisation können sichere Faxe oder elektronische Nachrichten dem DPC vorlegen, um neuen Mitgliedern Titel und Faxdurchwahl zuzuordnen, den Titel oder die Faxdurchwahl eines Mitglieds zu aktualisieren oder nicht mehr aktuelle Mitglieder zu löschen.

[0647] Wenn ein Individuum aus dem Organigramm gelöscht wird, inaktiviert das DPC die Durchwahlnummer für ein Jahr. Dies gibt dem Individuum ausreichend Zeit, vertraute Personen davon zu informieren, dass es nicht länger vertrauliche Faxe unter dieser Durchwahl empfangen kann, so dass die Organisation niemanden unter der Durchwahl irrtümlicherweise aktivieren kann, der Faxe empfangen könnte, die für ihn nicht bestimmt

sind.

[0648] Die EDD verwaltet eine Archivdatenbank, die Kopien von Dokumenten- und Empfängereinträgen enthält, wenn diese vom Absender oder einem der Empfänger des Dokuments angefordert werden. Die Archivdatenbank wird periodisch auf CD-ROM übertragen.

1.5.24.3. Datenbankschema

[0649] Die EDD besitzt drei Eintragtypen:
DocumentRecord: (Dokumenteneintrag)
documentNumber = int8
senderId = int4
documentFax = fax
documentText = text
messageKey = int8
status = int1
RecipientRecord: (Empfängereintrag)
documentNumber = int8
recipientId = int3
recipientFaxNumber = char12
recipientFaxExtension = char8
recipientEmailAddr = text
receivedBy = int4
lastModified = time
deliveryStatus = int1
contractStatus = 1
ArchiveRequestRecord: (Archivanfrageeintrag)
biometricId = int4
documentNumber = int8
requestorFaxNumber = char12
requestorFaxExtension = char8
requestorEmailAddr = text
OrganizationRecord: (Organisationseintrag)
biometricId = int4
registeredBy = int4
company = text
title = text
faxNumber = char12
faxExtension = char8
emailAddr = text
activeDate = time
privs = int2
status = int1

[0650] Es gibt die folgenden Möglichkeiten für das Dokumenteneintrag-Statusfeld:
0: unvollständig
1: OK

[0651] Es gibt die folgenden Möglichkeiten für das Empfängereintrag-Zustellstatusfeld:
0: unvollständig
1: benachrichtigt
2: abgewiesen
3: abgerufen
4: ungesichert abgerufen
5: besetzt

[0652] Es gibt die folgenden Möglichkeiten für das Empfängereintrag-Verstragsstatusfeld:
0: nicht vorhanden
1: angenommen
2: abgewiesen

[0653] Es gibt de folgenden Möglichkeiten für das Organisationseintrag-Statusfeld:
0: aktiv
1: suspendiert

[0654] Das Organisationseintrag-privs**-Feld dient zur Anzeige, welche Privilegien das DPC diesem Individuum zugesteht:
0: Registrierung

[0655] Den Schlüssel für die Dokumenten-, Empfänger- und Archivabrufeinträge bildet documentNumber. Den Schlüssel für die Organisationseinträge bildet biometricId. Die EDD verwaltet sekundäre Indizes im Dokument-senderId-Feld, im Empfänger-recipientId-Feld sowie im Organisations-Unternehmensnamen- und im Titelfeld.

1.5.24.4. Datenbankgröße

[0656] Die Speicheranforderungen der EDD hängen vor allem von der Anzahl an Faxseiten ab, die gespeichert werden müssen, da E-Mail-Nachrichten im Vergleich zu Faxseiten relativ klein sind. Jede Faxseite erfordert etwa 110 KB Speicher. Wenn man von 4 Seiten pro Fax und 2 Faxen pro Person pro Tag sowie von 30 Millionen Faxgeräten ausgeht, benötigt die EDD 24 GB Speicher, um die Tagesmenge an Faxnachrichten zu bewältigen.

1.5.24.5. Sicherheit

[0657] Dokumente werden in verschlüsselter Form – die Verschlüsselung erfolgt unter Anwendung des BIA-Verschlüsselungsmechanismus – an das System geschickt und von diesem abgeschickt. Der Verschlüsselungsschlüssel ist jedoch in der gleichen Datenbank gespeichert wie das Dokument. Das Dokument bleibt in seiner verschlüsselten Form, um unbeabsichtigte Offenlegung zu verhindern, doch Individuen, denen die Sicherheit von im System gespeicherten Dokumenten ein besonderes Anliegen ist, sollten selbst Vorkehrungen für eine zusätzliche Verschlüsselung treffen.

1.5.24.6. Nachrichtenbandbreite

[0658] Jede Faxseite erfordert etwa 110 kB – dies bedeutet, dass eine T1-Verbindung mit einem Durchsatz von 1,54 MB pro Sekunde etwa 1,75 Faxseiten pro Sekunde bewältigen kann.

1.5.25. Datenbank für elektronische Signaturen

1.5.25.1. Zweck

[0659] Die ESD authentifiziert und verfolgt alle durch das System generierten elektronischen Signaturen.

1.25.5.2. Nutzung

[0660] Individuen, die Mitglieder des Systems sind, legen für das Dokument einen 16-Byte-„Message Digest" sowie Biometrik-PICs vor und erhalten eine „digitale Signatur", die für immer im System präsent bleibt. Diese digitale Signatur codiert den Namen des Individuums, seinen biometrischen Identifizierungscode, die autorisierte Signatureintragnummer, den Dokumententitel sowie den Zeitstempel zum Zeitpunkt der Signatur des Dokuments.

[0661] Um eine Signatur zu verifizieren, wird ein Message Digest für das Dokument z. B. mittels MD5 von RSA berechnet und gemeinsam mit den Signaturmarkierungen des Dokuments versendet. Die ESD überprüft die Signaturmarkierungen und validiert die gerade eben berechnete Message Digest durch Vergleich mit der in der Datenbank gespeicherten Message Digest.

1.5.25.3. Datenbankschema

[0662] Das Schema für den Eintrag betreffend die elektronische Signatur sieht folgendermaßen aus:
ElectronicSignature: (elektronische Signatur)
signatureNumber = int4
signer = int4

documentName = text
checksum = int16
date = time

[0663] Der „Signer" (Signatar) ist der biometrische Identifizierungscode für das das Dokument signierende Individuum. Der Eintrag zur elektronischen Signatur ist durch die signatureNumber gehasht.

1.5.25.4. Datenbankgröße

[0664] Pro 1 GB Sekundärspeicher speichert die ESD 27 Millionen Einträge (jeder Eintrag umfasst etwa 32 Bytes).

1.5.25.5. Abhängigkeiten

[0665] Die ESD ist von der biometrischen Identifizierung des Signers abhängig. Da diese Signatur im Wesentlichen für immer gültig bleibt, werden die ESD-Einträge nicht entfernt, wenn das System den individuellen biometrischen Datenbankeintrag des Signers löscht. Es ist zu beachten, dass dies erforderlich macht, dass die IBD eine biometrische Identifizierung niemals wieder verwendet.

1.5.26. Fernhändlerdatenbank

1.5.26.1. Zweck

[0666] Die RMD speichert Informationen über Händler, die Güter oder Dienste über Telefon, Kabel-TV-Netze oder das Internet anbieten. Jede von einem Individuum mit einem ordnungsgemäß ausgerüsteten Endgerät abgeschickte Bestellung wird durch das Bestellungsendgerät des Händlers an das System geleitet.

1.5.26.2. Nutzung

[0667] Sobald die Fern-Transaktionsautorisierung des Individuums eingelangt und der MAC durch das DPC validiert ist, wird der Händlercode mit dem Händlercode in der RMD verglichen. Der Händlercode – die Telefonnummer, das Händlerprodukt-Credential oder die Internetadresse – existiert im RMD-Eintrag unter dem korrekten Händleridentifizierungscode; andernfalls bricht das DPC die Anfrage ab und schickt eine auf „ungültiger Händlercode" lautende Fehlermeldung an das absendende BIA-Endgerät zurück.

1.5.26.3. Datenbankschema

[0668] Das Schema für den Fernhändlereintrag sieht folgendermaßen aus:
RemoteMerchant: (Fernhändler)
merchantId = int4
merchantCode = char16
merchantType = int1
publicKey = int16

[0669] Es bestehen die folgenden Möglichkeiten für den Fernhändler-Händlertyp:
0: Telefon
1: CATV
2: Internet

[0670] Der merchantId und der merchantCode sind beides primäre Schlüssel. Kein RMD-Eintrag besitzt die gleiche Kombination aus merchantId und merchantCode.

1.5.26.4. Datenbankgröße

[0671] Wenn man von etwa 100.000 Fernhändlern ausgeht, braucht die RMD etwa 24 Bytes pro Sekunde für insgesamt etwa 2,4 MB benötigten Speicher.

1.5.26.5. Abhängigkeiten

[0672] Die RMD ist in keiner Weise direkt von anderen DPC-Komponenten abhängig.

1.5.27. Systemperformance

[0673] Der wesentliche Performanceindikator ist die Anzahl an Finanztransaktionen, die das DPC pro Sekunde bearbeitet.

In der GM

1. Das MACM überprüft den MAC (lokal)
2. Das SNM überprüft die Folgenummer (Netzwerknachricht)
3. Das MDM entschlüsselt den Biometrik-PIC-Block (lokal)
4. Die IBD-Maschine wird gefunden (lokal)
5. Die Identifizierungsanfrage wird an die IBD-Maschine gesendet (Netzwerknachricht)

In der IBD-Vorrichtung

6. Alle IBD-Einträge für den PIC werden abgerufen (x Suchen und x Lesen, wobei x die Seitenanzahl ist, die zur Speicherung der biometrischen Einträge erforderlich ist).
7. Jeder Eintrag wird mit seiner primären biometrischen Eingabe verglichen (y/2 ms, wobei y die Anzahl abgerufener Einträge ist).
8. Wenn keine vernünftige Übereinstimmung besteht, ist Schritt 9 zu wiederholen, doch ein Vergleich mit der sekundären biometrischen Eingabe zu ziehen (z*y/2 ms, wobei y die Anzahl der abgerufenen Einträge ist und z die Wahrscheinlichkeit ist, dass keine Übereinstimmung gefunden wird).
9. Die Prüfsummen-Warteschlange des am besten übereinstimmenden IBD-Eintrags ist zu aktualisieren, und es ist auf mögliche Wiedergabeangriffe zu achten (1 Suchen, 1 Lesen und 1 Schreiben).
10. Zurücksenden des am besten übereinstimmenden IBD-Eintrags oder Fehlermeldung, wenn die Übereinstimmung nicht nah genug ist (Netzwerknachricht).

In der GM

11. Autorisierung der Anfrage mit einem externen Prozessor (Netzwerknachricht)
12. Die GM verschlüsselt die Antwort und versieht sie mit dem MAC (lokal)
13. Zurücksenden des Antwortpakets (Netzwerknachricht)

Gesamte Plattenkosten

[0674]

x*(s + r) + y/2*(1 + z) + s + r + w + 5*n
= (x + 1)*(s + r) + y/2*(1 + z) + w + 5*n

[unter der Annahme, dass x 20 ist, y 30 ist, z 5% ist; s = 10 ms, r = 0 ms, w = 0 ms, n = 0 ms]
= 21*10 ms + 15*1,05 ms
= 226 ms
= 4,4 TPS
[unter der Annahme, dass x 10 ist, y 15 ist, z 5% ist; s = 10 ms, r = 0 ms, w = 0 ms, n = 0 ms]
= 11*10 ms + 7,5*1,05 ms
= 118 ms
= 8,4 TPS
[unter der Annahme, dass x 1 ist, y 1 ist, z 5% ist; s = 10 ms, r = 0 ms, w = 0 ms, n = 0 ms]
= 2*10 ms + 1/2*1,05 ms
= 21 ms
= 47 TPS

[0675] Die Sicherungs-ID-Vorrichtung verarbeitet ebenfalls Anfragen, wodurch der effektive TPS-Wert verdoppelt wird.

Schlimmster Fall (2 Vorrichtungen im Einsatz)

Individuen pro PIC	TPS
30	8
15	16
1	94

Durchschnittlicher Fall (2 Vorrichtungen im Einsatz)

Individuen pro PIC	TPS
30	88
15	168
1	940

Bester Fall (40 Vorrichtungen im Einsatz)

Individuen pro PIC	TPS
30	176
15	336
1	1880

[0676] Die obigen Ausführungen stellen nur ein Beispiel einer Systemkonfiguration dar, so wie sie in einer kommerziell vernünftigen Weise implementiert sein könnte. Es ist jedoch denkbar, die Erfindung in ganz anderer Weise zu konfigurieren – die Verwendung von schnelleren und mehr Computern o. dgl. ist möglich.

1.6. Endgerät-Protokollflussdiagramm

[0677] Die folgenden Protokollflussdiagramme beschreiben die Interaktionen zwischen bestimmten Endgeräten, dem DPC, der angefügten BIA und anderen Teilnehmern wie z. B. dem Lastschrift/Gutschrift-Prozessor usw.

1.6.1. Einzelhandelskassenendgerät (RPT)

[0678] In diesem Fall kommuniziert ein RPT mit einer Einzelhandels-BIA und dem DPC, um eine Transaktion zu autorisieren. Der Transaktionsbetrag ist 452,33, das Konto des Individuums ist 4024-2256-5521-1212, der Händlercode ist 123456, und der private Code des Individuums lautet „Ich bin davon ganz überzeugt."
RPT → BIA Sprache einstellen <Englisch>
BIA → RPT OK
RPT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → RPT OK
RPT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt PIC ein und drückt dann <enter>
BIA → RPT OK
RPT → BIA Kontonummer erhalten <40>
BIA/LCD: <Geben Sie nun Ihren Kontoindexcode ein und drücken Sie dann <enter>>
Individuum gibt Code ein und drückt dann <enter>

BIA → RPT OK
RPT → BIA Betrag validieren <452,33> <40>
BIA/LCD: <Betrag 452,33 OK?>
Individuum gibt OK ein
BIA → RPT OK
RPT → BIA Register zuordnen <1> <123456>
BIA → RPT OK
RPT → Nachricht erstellen <Transaktion>
BIA → RPT <Transaktionsanfrage-Nachricht>
BIA → RPT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
RPT → DPC <Transaktionsanfrage-Nachricht>
DPC: biometrische Eingabe validieren, Kontonummer aufrufen → 4024-2256-5521-1212
DPC → VISA <Autorisieren von 4024-2256-5521-1212 452,33 123456>
VISA → DPC <OK 4024-2256-5521-1212 452,33 123456 Autorisierungscode>
DPC: privaten Code erhalten
DPC → RPT <Transaktionsantwort-Nachricht>
RPT → BIA Antwort zeigen <Transaktionsantwort-Nachricht> <8>
BIA/LCD: <Transaktion OK: Ich bin ganz davon überzeugt>
BIA → RPT <OK <Autorisierungscode>>
RPT: druckt Quittung mit darauf vermerktem Autorisierungscode aus

1.6.2. Internet-Kassenendgerät

[0679] In diesem Fall kommuniziert ein IPT mit einer Standard-BIA und dem DPC, um eine Transaktion zu genehmigen. Der Transaktionsbetrag ist 452,33, die Kontonummer des Individuums ist 4024-2256-5521-1212, der Internethändler befindet sich bei merchant.com, sein Händlercode ist 123456, und der private Code des Individuums lautet „Ich bin ganz davon überzeugt."
IPT → mechant.com <Senden Sie mir den Händlercode, wenn die Ressourcen verfügbar sind>
merchant.com → IPT <OK 123456 merchant.com-public-key>
IPT erstellt Session Key, verschlüsselt mit merchant.com-public-key
IPT → merchant.com <Session Key>

[0680] Alle nachfolgenden Kommunikationen mit dem Händler werden vom Session Key verschlüsselt.
merchant.com → IPT <Preis- und Produktinformation>
IPT/Schirm: zeigt Preis- und Produktinformation an
Individuum: wählt Produkt „Fruchttorte, Preis 45,33" aus
IPT → BIA Sprache einstellen <Englisch>
BIA → IPT OK
IPT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → IPT OK
IPT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt PIC ein und drückt dann <enter>
BIA → IPT OK
IPT → BIA Kontonummer erhalten <40>
BIA/LCD: <Geben Sie nun Ihren Kontoindexcode ein und drücken Sie dann <enter>>
Individuum gibt Code ein und drückt dann <enter>
BIA → IPT OK
IPT → BIA Betrag validieren <45,33> <40>
BIA/LCD: <Betrag 45,33 OK?>
Individuum gibt OK ein
BIA → IPT OK
IPT → BIA Register zuordnen <1> <123456>
BIA → IPT OK
IPT → BIA Register zuordnen <2> <merchant.com>
BIA → IPT OK
IPT → BIA Register zuordnen <3> <Fruchttorte>

BIA → IPT OK
IPT → BIA Nachricht erstellen <Ferntransaktion>
BIA → IPT <Ferntransaktionsanfrage-Nachricht>
BIA → IPT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
IPT → merchant.com <Ferntransaktionsanfrage-Nachricht>
merchant.com → gesicherte Verbindung mit DPC mittels DPC Public Key
merchant.com → DPC <Ferntransaktionsanfrage-Nachricht>
DPC: biometrische Eingabe validieren, Kontonummer abrufen → 4024-2256-5521-1212
DPC: Internet merchant.com mit Code 123456 validieren
DPC → VISA: <Autorisieren von 4024-2256-5521-1212 45,33 123456>
VISA → DPC: <OK 4024-2256-5521-1212 45,33 123456 Autorisierungscode>
DPC: privaten Code erhalten
DPC → merchant.com <Transaktionsantwort-Nachricht>
merchant.com speichert Autorisierungscode
merchant.com → IPT <Transaktionsantwort-Nachricht>
IPT → BIA Antwort zeigen <Transaktionsantwort-Nachricht> <8>
BIA/LCD: <Transaktion OK: Ich bin ganz davon überzeugt>
BIA → IPT <Transaktion OK>

1.6.3. Internetbankschalter-Endgerät

[0681] In diesem Fall kommuniziert ein ITT mit einer Standard-BIA, dem DPC und dem Internetserver einer Bank, um Routine- und Nicht-Routine-Home-Banking-Vorgänge durchzuführen. Es ist zu beachten, dass das DPC in der tatsächlichen Bestätigung von Transaktionen nicht involviert ist, jedoch dafür verantwortlich zeichnet, einen validen Satz an Netzwerk-Credentials zu schaffen und die Kommunikationsleitung zur Bank zu sichern.
ITT → bank.com <Senden Sie mir Bankleitzahl, wenn Ressourcen verfügbar sind>
bank.com → ITT <OK 1200>
ITT → BIA Sprache einstellen <Englisch>
BIA → ITT OK
ITT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → ITT OK
ITT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt PIC ein und drückt dann <enter>
BIA → ITT OK
RPT → BIA Kontonummer erhalten <40>
BIA/LCD: <Geben Sie nun Ihren Kontoindexcode ein und drücken Sie dann <enter>>
Individuum gibt Code ein und drückt dann <enter>
BIA → ITT OK
ITT → BIA Register zuordnen <1> <1200> (Bankleitzahl)
BIA → ITT OK
ITT → BIA Register zuordnen <2> <bank.com>
BIA → ITT OK
ITT → BIA Register zuordnen <3> <ITT.port.bank.com.port> (TCP/IP-Adressen)
BIA → ITT OK
ITT → Nachricht erstellen <net credential>
BIA → ITT <Netzwerk-Akkreditiv-Anfrage>
BIA → ITT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
ITT → DPC <Netzwerk-Credential-Anfrage>
DPC: biometrische Eingabe validieren, Akkreditiv erstellen (Zeit, Konto, Bank)
DPC: privaten Code erhalten
DPC → ITT <Netzwerk-Akkreditiv-Antwort>
ITT → BIA Antwort zeigen <Netzwerk-Akkreditiv-Antwort>
BIA entschlüsselt Antwort, überprüft Antwort
BIA/LCD: <Akkreditiv OK: Ich bin ganz davon überzeugt>

BIA entschlüsselt Akkreditiv, Session Key, Challenge Key mit Public Key der Bank
BIA → ITT <Nachricht betreffend Anfrage zu gesicherter Verbindung>
BIA → ITT <Session Key>
BIA → ITT OK
BIA/LCD: <sichere Verbindung zu bank.com im Gang>
ITT → bank.com <Nachricht betreffend Anfrage zu gesicherter Verbindung>
bank.com entschlüsselt mit Private Key, validiert Akkreditiv, verwendet Shared Key
bank.com → ITT <OK>

[0682] Weitere Transaktionen über die ITT → bank.com-Verbindungen werden alle mit dem ITT/Bank Session Key durch das ITT verschlüsselt.

[0683] Alle Transaktionen, die von der Bank als Nicht-Routine-Transaktionen eingestuft werden, müssen vom Individuum mittels des Challenge-Response-Mechanismus der BIA bestätigt werden.

[0684] Der Challenge-Response-Mechanismus steht nur zur Verfügung, während die BIA im Zustand der „sicheren Verbindung" verharrt.
bank.com → ITT <validieren <Anfrage validieren>>
ITT → BIA privaten Code validieren <verschlüsselte Validierungsanfrage>
BIA entschlüsselt Challenge-Abschnitt und zeigt ihn an
BIA/LCD: <Geben Sie bitte OK ein: Überweisung von 12.420,00 auf 1023-3302-2101-1100>
Individuum gibt OK ein
BIA verschlüsselt Antwort erneut mit Challenge Key
BIA/LCD: <sichere Verbindung zu bank.com im Gang>
BIA → ITT <OK <verschlüsselte Validierungsantwort>>
ITT → bank.com <verschlüsselte Validierungsantwort>

1.6.4. Endgerät für elektronische Signaturen

[0685] In diesem Fall kommuniziert ein EST mit einer Standard-BIA und dem DPC, um die digitale Signatur zu erstellen. Der private Code des Individuums ist „Ich bin ganz davon überzeugt", und das zu signierende Dokument nennt sich „Der Kaperbrief".
CET → BIA Sprache einstellen <Englisch>
BIA → CET OK
CET → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → CET OK
CET → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt seinen PIC ein und drückt dann <enter>
BIA → CET OK
CET → BIA Dokument <Kaperbrief> validieren <40>
BIA/LCD: <Dokument „Kaperbrief" OK>
Individuum gibt OK ein
BIA → CET OK
CET → BIA Register zuordnen <1> <Dokument MD5 Wert>
BIA → CET OK
CET → Nachricht erstellen <Vorlage der Signatur>
BIA → CET <Anfrage zu elektronischer Signatur>
BIA → CET OK
BIA/LCE: <Ich spreche mit zentralem DPC>
CET → DPC <Anfrage zu elektronischer Signatur>
DPC: biometrische Eingabe validieren, Signatur erstellen, Signaturtextcode zurücksenden
DPC: privaten Code erhalten
DPC → CET <Antwort zu elektronischer Signatur>
CET → BIA Antwort zeigen <Antwort zu elektronischer Signatur> <8>
BIA/LCD: <Dokument OK: Ich bin ganz davon überzeugt>
BIA → CET <OK <Signaturtextcode>>

1.6.5. Endgerät für zertifizierte E-Mails

[0686] In diesem Fall kommuniziert ein CET mit einer Standard-BIA und dem DPC; um eine zertifizierte E-Mail-Nachricht zu übermitteln. Der private Code des Individuums lautet „Ich bin ganz davon überzeugt", und der Name des Dokuments ist „Postkapitän".
CET → BIA Sprache einstellen <Englisch>
BIA → CET OK
CET → BIA biometrische Eingabe erhalten <20>
BIA → LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → CET OK
CET → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt seinen PIC ein und drückt dann <enter>
BIA → CET OK
CET → BIA Dokument <Postkapitän> validieren <40>
BIA/LCD: <Dokument „Postkapitän" OK?>
Individuum gibt OK ein
CET/Schirm: <Empfängerliste?>
Individuum gibt <fred@telerate.com joe@reuters.com> ein
CET → BIA Register zuordnen <1> <fred@telerate.com joe@reuters.com>
BIA → CET OK
CET → Nachricht <Dokumentvorlage> erstellen
BIA → CET <Anfrage zu elektronischer Dokumentvorlage>
BIA → CET OK
BIA/LCD: <Ich spreche mit zentralem DPC>
CET → DPC <Anfrage zu elektronischer Dokumentenvorlage>
DPC: biometrische Eingab validieren, Nachricht erstellen, Nachricht Nr. 001234 zurücksenden
DPC: privaten Code erhalten
DPC → CET <Antwort auf elektronische Dokumentvorlage>
CET → BIA Antwort zeigen <Antwort auf elektronische Dokumentvorlage> <8>
BIA/LCD: <Dokument OK: ich bin ganz davon überzeugt>
BIA → CET <Dokument OK <1234>>
CET → DPC <Anfrage zu elektronischen Dokumentdaten, 1234, Abschnitt 1, unvollständig>
DPC → CET <Antwort auf elektronische Dokumentdaten, unvollständig>
CET → DPC <Anfrage zu elektronischen Dokumentdaten, 1234, Abschnitt 2, unvollständig>
DPC → CET <Antwort auf elektronische Dokumentdaten, unvollständig>
CET → DPC <Anfrage zu elektronischen Dokumentdaten, 1234, Abschnitt 3, unvollständig>
DPC → CET <Antwort auf elektronische Dokumentdaten, unvollständig>
CET → DPC <Anfrage zu elektronischen Dokumentdaten, 1234, Abschnitt 4, erledigt>
DPC → CET <Antwort auf elektronische Dokumentdaten, Spur 1234.1 1234.2>
DPC → fred@telerate.com <E-Mail 1234.1 Nachricht eingetroffen>
DPC → joe@reuters.com <E-Mail 1234.2 Nachricht eingetroffen>
mailer@telerate.com → DPC <Benachrichtigung E-Mail für 1234.1 empfangen>
DPC → sender@company.com <E-Mail 1234.1 Empfänger benachrichtigt>
mailer@reuters.com → DPC <Benachrichtigung E-Mail für 1234.2 empfangen>
DPC → sender@company.com <E-Mail 1234.2 Empfänger benachrichtigt>

[0687] [Im CET von Fred: Fred sieht die E-Mail-Nachricht „Nachricht eingetroffen" und beschließt, die Nachricht abzurufen.]
CET → BIA Sprache einstellen <Englisch>
BIA → CET OK
CET → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf den Scanner
BIA → CET OK
CET → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein>
Individuum gibt seinen PIC ein und drückt dann <enter>>
BIA → CET OK

CET → BIA Register zuordnen <1> <1234.1>
BIA → CET OK
CET → Nachricht erstellen <Dokumentabruf>
BIA → CET <Anfrage zu elektronischem Dokumentabruf>
BIA → CET OK
BIA/LCD: <Ich spreche mit zentralem DPC>
CET → DPC <Anfrage zu elektronischem Dokumentabruf>
DPC: biometrische Eingabe validieren, 1234.1 nachsehen
DPC: privaten Code erhalten
DPC → CET <Antwort auf elektronischen Dokumentabruf>
CET → BIA Antwort zeigen <Antwort auf elektronischen Dokumentabruf> <8>
BIA/LCD: <Dokument OK: Ich bin ganz davon überzeugt>
BIA → CET <Dokument OK <Nachrichtenschlüssel>>
CET/Schirm: entschlüsseln, dann Dokument zeigen

1.6.6. Endgerät für sichere Faxnachrichten

[0688] In diesem Fall kommuniziert ein SFT mit einem BIA/catv und dem DPC, um sichere Faxnachrichten zu übermitteln.
SFT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA → SFT OK
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt PIC ein und drückt dann <enter>
SFT → BIA Pin setzen <40>
BIA/LCD: <Bitte geben Sie Ihren Titelindex ein und drücken Sie dann <enter>>
Individuum gibt Titelindex ein und drückt dann <enter>>
SFT → BIA Titelindexcode setzen <40>
BIA → SFT OK
SFT/Schirm: <Empfänger? (* für Durchwahl anfügen, # am Ende)>
Individuum gibt <1 510 944-6300*525#> ein
SFT/Schirm <Empfänger? (* für Durchwahl anfügen, # am Ende)>
Individuum gibt <1 415-877-7770> ein
SFT/Schirm: <Empfänger? (* für Durchwahl anfügen, # am Ende)>
Individuum gibt <#> ein
SFT → BIA Register zuordnen <1> <15109446300*525 14158777770>
BIA → SFT OK
SFT → Nachricht erstellen <Dokumentvorlage>
BIA → SFT <Anfrage zur Vorlage sicherer Faxnachrichten>
BIA → SFT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
SFT → DPC <Anfrage zur Vorlage sicherer Faxnachrichten>
DPC: biometrische Eingabe validieren, Nachricht erstellen, Nachricht Nr. 001234 zurücksenden
DPC: privaten Code erhalten
DPC → SFT <Antwort auf Vorlage sicherer Faxnachrichten>
SFT → BIA Antwort zeigen <Antwort auf Vorlage sicherer Faxnachrichten> <10>
BIA/LCD: <Dokument OK: Ich bin ganz davon überzeugt>
BIA → SFT <Dokument OK <001234>>
SFT → DPC <Anfrage zu sicheren Faxdaten, 1234, Abschnitt 1, unvollständig>
DPC → SFT <Antwort betreffend sichere Faxdaten, unvollständig>
SFT → DPC <Anfrage zu sicheren Faxdaten, 1234, Abschnitt 2, unvollständig>
DPC → SFT <Antwort betreffend sichere Faxdaten, unvollständig>
SFT → DPC <Anfrage zu sicheren Faxdaten, 1234, Abschnitt 3, unvollständig>
DPC → SFT <Antwort betreffend sichere Faxdaten, unvollständig>
SFT → DPC <Anfrage zu sicheren Faxdaten, 1234, Abschnitt 4, erledigt>
DPC → SFT <Antwort betreffend sichere Faxdaten>
DPC → Faxverbindung 15109446300
DPC → SFT6300 <Faxdeckblatt „Sam Spade" von „Fred Jones" 1234.1 4 Seiten eingetroffen>
DPC → Verbindung trennen

DPC → Faxverbindung 14158777770
DPC → SFT7770 <Faxdeckblatt „John Jett" von „Fred Jones" 1234.2 4 Seiten eingetroffen>
DPC → Verbindung trennen

[0689] [Im SFT von Sam: Sam sieht die Ankunft des Faxdeckblatts von Fred und leitet die Abrufung des Dokuments vom DPC mittels des Verfolgungscodes 1234.1 ein.]
SFT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum (Sam) legt seinen Finger auf Scanner
BIA → SFT OK
SFT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum (Sam) gibt seinen PIC ein und drückt dann <enter>
BIA → SFT OK
SFT → BIA Register zuordnen <1> <1234.1>
BIA → SFT OK
SFT → Nachricht erstellen <Dokumentabruf>
BIA → SFT <Anfrage zum Abruf sicherer Faxnachrichten>
BIA → SFT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
SFT → DPC <Anfrage zum Abruf sicherer Faxnachrichten>
DPC: biometrische Eingabe validieren, 1234.1 nachsehen, Biometrik-PIC = Sam Spade verifizieren
DPC: privaten Code in Datenbank nachsehen
DPC → SFT <Antwort auf Abruf sicherer Faxnachriten>
SFT → BIA Antwort zeigen <Antwort auf Abruf sicherer Faxnachrichten> <8>
BIA → SFT <Dokument OK: Ich bin ganz davon überzeugt <Nachrichtenschlüssel>>
SFT/Schirm: <Dokument OK: Ich bin ganz davon überzeugt>
SFT/Schirm: Fax drucken

1.6.7. Biometrisches Registrierungsendgerät

[0690] In diesem Fall kommuniziert ein BRT mit einer Registrierungs-BIA und dem DPC; um ein Individuum im System zu registrieren.
BRT → BIA Sprache einstellen <Englisch>
BIA → BRT OK
BRT → BIA biometrische Eingabe erhalten <20> <erste>
BIA/LCD: <Bitte legen Sie ERSTEN Finger auf das beleuchtete Feld>
Individuum legt seinen ersten Finger auf Scanner
BIA → BRT OK
BRT → BIA biometrische Eingabe erhalten <20> <zweite>
BIA/LCD: <Bitte legen Sie ZWEITEN Finger auf das beleuchtete Feld>
Individuum legt seinen zweiten Finger auf Scanner
BIA → BRT OK
BRT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt 123456 ein und drückt dann <enter>
BIA → BRT OK
BRT → BIA Nachrichtenschlüssel erhalten
BIR → BRT <OK <Nachrichtenschlüssel>>
BRT/Schirm: <Name:>
Vertreter gibt <Fred G. Shultz> ein
BRT/Schirm: <Adresse:>
Vertreter gibt <1234 North Main> ein
BRT/Schirm: <Postleitzahl:>
Vertreter gibt <94042> ein
BRT/Schirm: <privater Code:>
Vertreter fragt Individuum und gibt dann <Ich bin ganz davon überzeugt> ein>
BRT/Schirm: <Finanzkontoliste:>
Vertreter gibt <2, 1001-3001-1020-2011> (Kreditkarte) ein
Vertreter gibt <3, 1001-1002-0039-2212> (Girokonto) ein

BRT/Schirm: <Notfallskonto:>
Vertreter gibt <1, 1001-1002-0039-2212> (Notfall, Girokonto) ein
BRT → Nachricht erstellen <Registrierung>
BIA → BRT <Registrierungsanfragenachricht>
BIA → BRT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
BRT fügt mit Nachrichtenschlüssel verschlüsselte persönliche Information an Anfrage an
BRT → DPC Registrierungsanfragenachricht <verschlüsselte persönliche Information>
DPC: PIC 123456 verifizieren
DPC → BRT <Registrierungsantwortnachricht>
BRT → BIA Antwort zeigen <Registrierungsantwortnachricht> <8>
BIA/LCD: <Registrierung OK: Ich bin ganz davon überzeugt, 123456>
BIA → BRT <OK>

1.6.8. Kundendienstendgerät

[0691] In diesem Fall kommuniziert ein CST mit einer Standard-BIA und dem DPC, um Identität und Akkreditive eines Individuums zu verifizieren.
CST → BIA Sprache einstellen <Englisch>
BIA → CST OK
CST → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA → CST OK
CST → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt seinen PIC ein und drückt dann <enter>
BIA → CST OK
CST → BIA Nachrichtenschlüssel erhalten
BIA → CST <OK <Nachrichtenschlüssel>>
CST → Nachricht erstellen <Anfrage zu individueller Identität>
BIA → CST <Anfrage zu individueller Identität>
BIA → CST OK
BIA/LCD: <Ich spreche mit zentralem DPC>
CST → DPOC <Anfrage zu individueller Identität>
DPC: privaten Code, Privilegienstatus des Individuums erhalten
DPC → CST <Antwort auf individuelle Identität>
CST → BIA Antwort zeigen <Antwort auf individuelle Identität> <8>
BIA/LCD: <Identität OK: Ich bin ganz davon überzeugt>
BIA → CST <OK <Individuum-Name Privilegienstatus>>
CST: Privilegienstatus kontrollieren, um zu überprüfen, ob zur CST-Verwendung ausreichend

1.6.9. Ausstellerendgerät

[0692] In diesem Fall kommuniziert ein IT mit einer Standard-BIA und dem DPC, um einen Stapel von Anfragen betreffend Kontohinzufügungen und -löschungen zu autorisieren und an das DPC zu schicken. Der private Code des Individuums lautet „Ich bin ganz davon überzeugt", und die Bankleitzahl lautet 1200.
IT → BIA Sprache einstellen <Englisch>
BIA v IT OK
IT → BIA biometrische Eingabe erhalten <20>
BIA/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA v IT OK
IT → BIA Pin erhalten <40>
BIA/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum gibt seinen PIC ein und drückt dann <enter>
BIA → IT OK
IT v BIA Register zuordnen <1> <1200>
BIA → IT OK
IT → BIA Nachrichtenschlüssel erhalten

BIA → IT <Nachrichtenschlüssel>
BIA → IT OK
IT → BIA Nachricht erstellen <Ausstelleranfrage>
BIA → IT <Ausstellerbatch-Anfrage>
BIA → IT OK
BIA/LCD: <Ich spreche mit zentralem DPC>
IT → DPC <Ausstellerbatch-Anfrage> <mit Nachrichtenschlüssel verschlüsselter Ausstellerbatch>
DPC: biometrische Eingabe, Bankleitzahl 1200 validieren und mit BIA-Identifizierung vergleichen
DPC: privaten Code erhalten
DPC: mit Nachrichtenschlüssel Nachricht entschlüsseln, Ausstellerbatch ausführen
DPC → IT <Ausstellerbatch-Antwort>
IT → BIA Antwort zeigen <Ausstellerbatch-Antwort> <8>
BIA/LCD: <Stapel OK: Ich bin ganz davon überzeugt>
BIA → IT <OK>

1.6.10. Geldausgabeautomat

[0693] In diesem Fall kommuniziert ein Geldausgabeautomat mit einer integrierten ATM-BIA und dem DPC, um ein Individuum zu identifizieren und seine Bankkontonummer zu erhalten. Die Kontonummer des Individuums ist 2100-0245-3778-1201, die Bankleitzahl 2100 und der private Code des Individuums „Ich bin ganz davon überzeugt".
ATM → BIA biometrische Eingabe erhalten <20>
ATM/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA → ATM OK
ATM/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>
Individuum gibt in die ATM-Tastatur 123456 ein und drückt dann <enter>
ATM → BIA Pin setzen <123456>
BIA → ATM OK
ATM/LCD: <Geben Sie nun Ihren Kontoindexcode ein und drücken Sie dann <enter>>
Individuum gibt 2 ein und drückt dann <enter>
ATM → BIA Kontoindexcode setzen <2>
BIA → ATM OK
ATM → BIA Register zuordnen <1> <2100>
BIA → ATM OK
ATM → Nachricht erstellen <Kontozugriff>
BIA → ATM <Nachricht betreffend Kontozugriffsanfrage>
BIA → ATM OK
ATM/LED: <Ich spreche mit zentralem DPC>
ATM → DPC <Nachricht betreffend Kontozugriffsanfrage>
DPC: biometrische Eingabe validieren, Kontonummer abrufen → 2100-0245-3778-1201
DPC: privaten Code erhalten
DPC → ATM <Nachricht betreffend Kontozugriffsantwort>
ATM → BIA Antwort entschlüsseln <Nachricht betreffend Kontozugriffsantwort>
BIA → ATM <2100-0245-3778-1201> <kein Notfall> <Ich bin ganz davon überzeugt>
ATM/LCD: <Ich bin ganz davon überzeugt>

[0694] Zu diesem Zeitpunkt verfügt der Geldausgabeautomat über die Kontonummer, die er für die weiteren Vorgänge benötigt; er ruft dann die Informationen in Zusammenhang mit der Kontonummer auf und beginnt die Interaktion mit dem Individuum.

1.6.11. Telefonkassenendgerät

[0695] In diesem Fall kommuniziert ein PPT mit einer integrierten Telefon-BIA und dem Telefonhändler, um Informationen und zum Kauf angebotene Produkte sicher über das Telefon herunterzuladen. Der PIC des Individuums lautet 1234, der Kontoindexcode 1, die Händlertelefonnummer 1-800-542-2231, der Händlercode 123456 und die eigentliche Kontonummer 4024-2256-5521-1212.

[0696] Es ist zu beachten, dass das Telefon vor der Übergabe an das System die Vorwahl (1-800) von der Telefonnummer streicht.

Individuum ruft die Telefonnummer 18005422231 an
PPT → Verbindung zu Händler 18005422231
PPT → BIA Register zuordnen 1 <542231>
Verkäufer antwortet. Individuum sucht das Produkt „Fruchttorte" aus. Der Verkäufer lädt Informationen herunter.
Händler → PPT <123456 Fruchttorte 43,54>
PPT → BIA biometrische Eingabe erhalten <20>
Telefon/LCD: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA → PPT OK
Telefon/LCD: <Bitte geben Sie Ihren PIC ein und drücken Sie dann #>
Individuum drückt auf dem Tastenfeld 1234 und dann # oder * (enter)
PPT → BIA Pin setzen <1234>
BIA → PPT OK
Telefon/LCD; <Geben Sie nun Ihren Kontoindexcode ein>
Individuum gibt 1 ein und drückt dann <enter>
RPT → BIA Kontoindexcode setzen <1>
BIA → PPT OK
RPT → BIA Register zuordnen <2> <123456>
BIA → PPT OK
Telefon/LCD: <Drücken Sie #, wenn der Betrag 43,54 OK ist>
Individuum drückt # (ja)
PPT → BIA Betrag setzen <43,54>
BIA → PPT OK
PPT → Nachricht erstellen <Ferntransaktion>
BIA → PPT <Anfrage zur Ferntransaktion>
BIA → PPT OK
Telefon/LCD: <Ich spreche mit zentralem DPC>
PPT → Händler <Anfrage zu Telefontransaktion>
Händler → DPC sichere Verbindung zum DPC mittels DPC-Public Key
Händler → DPC <Anfrage zu Telefontransaktion>
DPC: biometrische Eingabe validieren, Kontonummer abrufen → 4024-2256-5521-1212
DPC: validieren, dass Händler 5422231 den Code 123456 besitzt
DPC → VISA <Autorisierung von 4024-2256-5521-1212 43,54 123456>
VISA → DPC <OK 4024-2256-5521-1212 43,54 123456 Autorisierungscode>
DPC: privaten Code erhalten
DPC → Händler <Transaktions-Antwortnachricht>
Händler überprüft Antwortcode
Händler → PPT <Transaktions-Antwortnachricht>
PPT → BIA Nachricht entschlüsseln <Transaktions-Antwortnachricht>
BIA → PPT <OK> <Ich bin ganz davon überzeugt> <Autorisierungscode>>
Telefon/LCD: <Signal> Transaktion OK: Ich bin ganz davon überzeugt.

1.6.12. Kabel-TV-Kassenendgerät

[0697] In diesem Fall kommuniziert ein CPT mit einer integrierten Kabel-TV-BIA und dem Kabel-TV-Händler, um Informationen und zum Kauf angebotene Produkte sicher über das Kabel-TV-Breitbandnetz herunterzuladen. Der PIC des Individuums lautet 1234, der Kontoindexcode 1, der Kanal 5, der Händlercode 123456 und die tatsächliche Kontonummer 4024-2256-552-1212.

[0698] Das Individuum schaltet das Fernsehgerät ein und sieht Kanal 5.
Händler → CPT <Fruchttorte 43,54 123456> (Sendung)
Indidivuum drückt auf seiner Fernbedienung die Taste „Kaufen"
CPT/TV: <Kauf von Fruchttorte um $ 43,54>
CPT → BIA biometrische Eingabe erhalten <20>
CPT/TV: <Bitte legen Sie Ihren Finger auf das beleuchtete Feld>
Individuum legt seinen Finger auf Scanner
BIA → CPT OK
CPT/TV: <Bitte geben Sie Ihren PIC ein und drücken Sie dann <enter>>
Individuum drückt 1234 auf dem Tastenfeld und dann die Taste „Kaufen"

CPT → BIA Pin setzen <1234>
BIA → CPT OK
CPT/TV <Geben Sie nun Ihren Kontoindexcode ein>
Individuum gibt 1 ein und drückt dann <enter>
RPT → BIA Kontoindexcode setzen <1>
BIA → CPT OK
RPT → BIA Register zuordnen <1> <Kanal 5, 15:30:20 PST>
BIA → RPT OK
CPT → BIA Register zuordnen <2> <123456>
BIA → CPT OK
CPT/TV: <Drücken Sie "Kaufen", wenn der Betrag 45,54 OK ist>
Individuum drückt „Kaufen"
CPT → BIA Betrag setzen <43,54>
BIA → CPT OK
CPT → Nachricht erstellen <Kabel-TV-Transaktion>
BIA → CPT <Anfrage zu Kabel-TV-Transaktion>
BIA → CPT OK
CPT/TV: <Ich spreche mit zentralem DPC>
CPT → CTV Zentrale <Anfrage zu Kabel-TV-Transaktion>
CTV Zentrale → Händler <Anfrage zu Kabel-TV-Transaktion>
Händler → DPC sichere Verbindung zu DPC mittels DPC-Public Key
Händler → DPC <Anfrage zu Kabel-TV-Transaktion>
DPC: biometrische Eingabe validieren, Kontonummer abrufen → 4024-2256-5521-1212
DPC: validieren, dass Händlerkanal 5 und aktuelle Sendung Code 123456 hat
DPC → VISA <Autorisierung von 4024-2256-5521-1212 43,54 123456>
VISA → DPC <OK 4024-2256-5521-1212 43,54 123456 Autorisierungscode>
DPC: privaten Code, Zustelladresse erhalten
DPC → Händler <Transaktions-Antwortnachricht>
Händler überprüft Antwortcode, trägt Zustelladresse ein
Händler → CTV Zentrale <Transaktions-Antwortnachricht>
CPT → BIA Nachricht entschlüsseln <Transaktions-Antwortnachricht>
BIA → CPT <OK <Ich bin ganz davon überzeugt> <Autorisierungscode>>
CPT/TV: <Signal> Transaktion OK: Ich bin ganz davon überzeugt.

[0699] Aus den obigen Ausführungen ergibt sich, wie die Ziele und Merkmale der Erfindung verwirklicht werden.

[0700] Erstens bietet die Erfindung ein Computeridentifizierungssystem, mit dem ein Benutzer nicht mehr ein physisches Objekt wie z. B. einen Token besitzen und vorlegen muss, um eine Systemzugriffsanfrage zu initiieren.

[0701] Zweitens stellt die Erfindung ein Computeridentifizierungssystem bereit, das die Identität eines Benutzers verifizieren kann (zum Unterschied von der Verifikation des Besitzes proprietärer Objekte und Informationen).

[0702] Drittens verifiziert die Erfindung die Identität eines Benutzers basierend auf einer oder mehreren seiner eindeutigen persönlichen physikalischen Eigenschaften.

[0703] Viertens bietet die Erfindung ein Identifizierungssystem, das praktisch, bequem und benutzerfreundlich ist.

[0704] Fünftens stellt die Erfindung ein System für den gesicherten Zugriff auf ein Computersystem zur Verfügung, das gegenüber betrügerischen Zugriffsversuchen seitens nicht-autorisierter Benutzer äußerst sicher ist.

[0705] Sechstens bietet die Erfindung ein Computeridentifizierungssystem, mit dem ein Benutzer Behörden informieren kann, dass eine bestimmte Zugriffsanfrage von einem Dritten durch Nötigung erzwungen wird, ohne dass dieser Dritte von dieser Benachrichtigung erfährt.

[0706] Siebtens stellt die Erfindung ein Identifizierungssystem zur Verfügung, das die Identifizierung des Ab-

senders und Empfängers einer elektronischen und/oder Faxnachricht ermöglicht.

[0707] Zwar wurde die Erfindung unter Bezugnahme auf ein bestimmtes Identifizierungssystem ohne Token und ein Verfahren zu seiner Verwendung beschrieben, doch ist zu beachten, dass zahlreiche Modifikationen der Vorrichtung und des Verfahrens möglich sind, ohne vom Schutzbereich der in den nachstehenden Patentansprüchen dargelegten Erfindung abzuweichen.

GLOSSAR

Account Index Code (Kontoindexcode)

[0708] Eine aus Ziffern bestehende oder alphanumerische Folge, die einem bestimmten Finanzkonto entspricht.

AID (Datenbank der autorisierten Individuen)

[0709] Authorized Individual Database: enthält die Liste von Individuen, die autorisiert sind, persönliche und Aussteller-BIA-Vorrichtungen zu verwenden.

AOD (Datenbank der Besitzer von Vorrichtungen)

[0710] Apparatus Owner Database: zentrale Aufbewahrungsstelle, die die geografischen und Kontaktinformationen über den Besitzer jeder BIA enthält.

ASCII (amerikanischer Standardcode für Informationsaustausch)

American Standard Code for Information Interchange

ATM (Geldausgabeautomat)

[0711] Automated Teller Machinery: verwendet codierte Information zur biometrischen Identität, um Zugriff auf ein Finanzverwaltungssystem zu erhalten (einschließlich der Geldausgabe- und Kontoverwaltungsfunktionen).

BIA (biometrische Eingabevorrichtung)

[0712] Biometric Input Apparatus: erfasst, codiert und verschlüsselt Informationen zur biometrischen Identität und stellt sie für Autorisierungen zur Verfügung. Es bestehen unterschiedliche Hardwaremodelle und Softwareversionen davon.

Biometric (Biometrik)

[0713] Durch das System vorgenommene Messung eines physischen Aspekts eines Individuums.

Biometric ID (biometrische Identifizierung)

[0714] Identifizierungsmerkmal, mit dem das System den biometrischen Eintrag eines Individuums eindeutig identifizieren kann (IRID – Individual Record ID, Identifizierung des individuellen Eintrags).

Bio-PIC Group (Bio-PIC-Gruppe)

[0715] Sammlung algorithmisch unähnlicher biometrischer Proben, die mit dem gleichen persönlichen Identifizierungscode verbunden sind.

BRT (biometrisches Registrierungsendgerät)

[0716] Biometric Registration Terminal: befindet sich in Bankfilialen. Die BRTs kombinieren biometrische Registrierungsinformationen mit einem vom Individuum ausgewählten PIN und ausgewählten persönlichen Informationen, um Individuen im System zu registrieren.

CBC (Geheimtextblockverkettung)

[0717] Cipher Block Chaining: ein Verschlüsselungsmodus für DES.

CCD (Ladungsspeicherelement)

Charged-Coupled Device

CET (Endgerät für zertifizierte E-Mails)

[0718] Certified Email Terminal: bedient sich der BIA; um Absender zu identifizieren, verschlüsselt Dokumente und sendet sie an das System. Das System bewahrt die einlangende Nachricht und verständigt den Empfänger von deren Empfang. Der Empfänger identifiziert sich, und dann wird das Dokument an den Empfänger übermittelt. Es erfolgt auch die Benachrichtigung an den Übermittler, sobald das Dokument abgesendet wurde. Das Dokument wird verifiziert und durch BIA-Verschlüsselung gesichert verschickt. Der Absender kann Anfragen zum Zustellstatus richten. Beide Teilnehmer müssen Systemmitglieder sein.

Commands (Befehle)

[0719] Ein Programm oder eine Subroutine im DPC, die eine spezifische Aufgabe erfüllt (aktiviert durch eine Anfragenachricht, die von einem mit BIA ausgestatteten Endgerät abgeschickt wird).

Contract Accept/Reject (Annahme/Abweisung von Verträgen)

[0720] Verfahren, durch das ein Individuum seinen Bio-PIC eingibt und das DPC anweist, die Annahme oder die Abweisung der in einem Dokument enthaltenen vertraglichen Bestimmungen durch das Individuum zu registrieren, welches Dokument über elektronisches Fax an dieses Individuum übermittelt wurde.

CPT (Kabel-TV-Kassenendgerät)

[0721] Cable-TV Point-of-Sale Terminal: kombiniert Monitoranzeige und eine digitale Simultaninformations-TV-Top-Cable-Box für Produktinformationen mit Produktvideo sowie mit einer durch die BIA steuerbaren Fernbedienung, die die Biometrik-PIN-Validierung unter Einsatz des CATV-Kommunikationsnetzes durchführt.

CST (Kundendienstendgerät)

[0722] Customer Service Terminal: ermöglicht dem System-Kundendienstpersonal mit variierenden Zugriffsniveaus (abhängig vom Zugriffsprivileg), Informationen über Individuen abzurufen und zu modifizieren, um Menschen mit Kontoproblemen zu helfen.

Data Sealing Step (Datenversiegelungsschritt)

[0723] Die Umwandlung von Klartext in verschlüsselten Text (als „Verschlüsselung" bezeichnet) in Kombination mit der verschlüsselten Prüfsummenbildung einer Nachricht, so dass Informationen in Klartext bleiben können, während gleichzeitig die Möglichkeit geschaffen wird, nachfolgende Modifikationen der Nachricht zu detektieren.

DES (digitaler Verschlüsselungsstandard)

[0724] Digital Encryption Standard: Standard für den kryptographischen Schutz digitaler Daten. Siehe Standard ANSI X3.92-1981

Determination (Bestimmung)

[0725] Status des während des Ausführungsschritts verarbeiteten Befehls.

DPC (Datenverarbeitungszentrum)

[0726] Data Processing Center, d. h. der Ort bzw. die Einrichtung, wo sich Hardware, Software und Personal befinden und der bzw. die das Ziel verfolgt, eine Multigigabyte große biometrische Identitätsdatenbank zu un-

terstützen. Ein DPC verarbeitet elektronische Nachrichten, von denen die meisten die Durchführung biometrischer Identitätskontrollen als Vorstufe für bestimmte andere Aktivitäten (Finanztransaktionen, Senden von Faxnachrichten oder von E-Mails usw.) vorsehen.

DSP (digitaler Signalprozessor)

[0727] Digital Signal Processor: eine Klasse integrierter Schaltungen, die sich auf mathematische Vorgänge spezialisieren, die im Bereich der Signalverarbeitungs-Applikationen erforderlich sind.

DUKPT (abgeleiteter eindeutiger Schlüssel pro Transaktion)

[0728] Derived Unique Key Per Transaction: siehe Standard ANSI/ABA X9.24-1992

EDD (Datenbank für elektronische Dokumente)

[0729] Electronic Document Database: zentrale Aufbewahrungsstelle für alle einlangenden Faxe und elektronischen Nachrichten, die von Individuen abzurufen sind.

Emergency Account Index (Notfallskontoindex)

[0730] Die von einem Individuum gewählte alphanumerische Ziffer oder Ziffernfolge, die im Falle des Zugriffs dazu führt, dass die Transaktion durch das System als Notfallstransaktion markiert wird, die möglicherweise falsche Bildschirmanzeigen und/oder die Benachrichtigung von Behörden nach sich zieht, dass ein Individuum dazu genötigt wurde, eine Übertragung oder Transaktion durchzuführen.

ESD (Datenbank elektronischer Signaturen)

[0731] Electronic Signature Database: zentrale Aufbewahrungsstelle mit allen MD5 und elektronischen Signaturen aller signierter Dokumente (bezogen auf Autorisierungsnummer).

EST (Endgerät für elektronische Signaturen)

[0732] Electronic Signature Terminal: bedient sich der BIA, um Individuen zu identifizieren, berechnet die Prüfsumme auf dem Dokument mittels Computer, sendet die Prüfsumme an das System; das System validiert die Prüfsumme, versieht sie mit einem Zeitstempel und speichert sie; ferner sendet es den Signaturcode zurück. Verwendet Internet als Übertragungsmedium. EST verifiziert auch Signaturen, die als Signaturcode und MD5-Berechnung vorliegen.

FAR (falsche Annahmerate)

[0733] Die statistische Wahrscheinlichkeit, dass die biometrische Eingabe eines Individuums irrtümlicherweise als biometrische Eingabe eines anderen Individuums identifiziert wird.

False Screen (falsche Bildschirmanzeige)

[0734] Anzeigen von Informationen, die absichtlich und unauffällig unpräzise sind, so dass eine nötigende Person nicht illegal präzise Daten über die Vermögenssituation eines Individuums erhält; die nötigende Person ist sich der Informationsänderung nicht bewusst.

FDDI

[0735] Fiber Digital Device Interface: Netzwerkgerät, das einen Lichtwellenleiter-Token-Ring verwendet.

FS (Feldtrennzeichen)

Field Separator

FW

[0736] Firewall Machine: Internet-lokaler Netzrouter, der den Verkehr in und aus dem DPC regelt.

GM

[0737] Gateway Machine (Vorrichtung): Zentrale Computer für die Verarbeitung in der DPC; auf ihr läuft ein Großteil der Software.

IBD (individuelle biometrische Datenbank)

[0738] Individual Biometric Database: zentrale Aufbewahrungsstelle für biometrische, Finanz- und andere persönliche Informationen. Anfragen an die biometrische Datenbank dienen dazu, die Identität für Transaktionsautorisierungen und Übertragungen zu verifizieren.

ID (Ausstellerdatenbank)

[0739] Issuer Database: zentrale Aufbewahrungsstelle mit den Institutionen, die Finanzkontonummern im System hinzufügen und löschen können.

IML (IBD-Maschinen-Liste)

[0740] IBD Machine Liste: Softwaremodul im DPC, das bestimmt, welche IBD-Maschinen für welche PIN-Codes verantwortlich sind.

Internet Merchant (Internethändler)

[0741] Einzelhändler, der über das elektronische Internet Güter oder Dienstleistungen an Konsumenten verkauft.

IPT (Internet-Kassenendgerät)

[0742] Internet Point-of-Sale-Terminal: Produkte und Händlercode aus dem Internet, BIA-Biometrik-PIN für Validierung, gesendet an das System über das Internet, Autorisierung/Bestellung/PO-Nr. weitergeleitet an Händler. Systemantwort auch über Internet, Anzeige der Ergebnisse auf Schirm.

Issuer (Aussteller)

[0743] Aussteller von Finanzkonten, damit Vermögen im DPC registriert werden kann.

Issuer Batch (Ausstellerbatch)

[0744] Eine Sammlung von „Hinzufügen"- und „Löschen"-Anweisungen, umfassend biometrische Identifizierungen, Finanzkonten und Kontoindexcodes (von einem Aussteller verifiziert und dem DPC vorgelegt).

IT (Ausstellerendgerät)

[0745] Issuer Terminal: sorgt für Batchverbindung zum System, damit Aussteller (ihre eigenen) Finanzkontonummern aus IBD-Einträgen eines bestimmten Individuums löschen oder diese den Einträgen hinzufügen können.

ITT (Internet-Bankschalterendgerät)

[0746] Internet Teller Terminal: autorisiert Netzwerksitzungen des Endgeräts mittels verschlüsseltem Akkreditiv, das vom DPC unter Verwendung von biometrischer Identifizierung erhalten wurde.

LCD (Flüssigkristallanzeige)

[0747] Liquid Crystal Display: Technologie zur Anzeige von Text.

MAC (Nachrichten-Authentifizierungscode)

[0748] Message Authentication Code: verschlüsselter Prüfsummenalgorithmus; der MAC bietet die Sicherheit, dass der Inhalt einer Nachricht nach der MAC-Berechnung nicht geändert wurde. Siehe Standard ANSI

X9.9-1986.

MACM (Nachrichten-Authentifizierungscode-Modul)

[0749] Message Authentication Code Module: Softwaremadul im DPC, das für MAC-Validierung und Generierung für abgehende und hereinkommende Pakete zuständig ist.

MDM (Nachrichten-Enschlüsselungsmodul)

[0750] Message Decrypt Module: Softwaremodul im DPC, das Pakete von einer und zu einer BIA ver- und entschlüsselt.

MPM (Nachrichten-Verarbeitungsmodul)

[0751] Message Processing Module: Softwaremodul im DPC, das die Verarbeitung von Anfragepaketen durchführt.

Network Credential (Netzwerk-Akkreditiv)

[0752] Sowohl das Individuum als auch die Bank werden vom DPC identifiziert, um das Netzwerk-Akkreditiv zu erstellen. Das Akkreditiv umfasst die Identifizierung des Individuums sowie den Verbindungskontext (d. h. die TCP/IP-Quell- und Zielanschlüsse). Das DPC erstellt ein Netzwerk-Akkreditiv mittels der Kontoidentifizierung des Individuums, der Tageszeit und der Bankleitzahl. Das DPC signiert dieses Akkreditiv unter Anwendung von Public Key-Verschlüsselung und des DPC-Private Key.

PFD (Datenbank über früheren Missbrauch)

[0753] Prior Fraud Database: zentrale Aufbewahrungsstelle für IBD-Einträge, mit denen Fälle vorherigen Systemmissbrauchs assoziiert sind. Die biometrische Eingabe jedes neuen Kunden wird mit allen PFD-Einträgen verglichen, um Wiederholungstätern Einhalt zu gebieten.

PGL (PIN-Gruppen-Liste)

[0754] PIN Group List: ein Softwaremodul im DPC, das für die Aufrechterhaltung der Konfiguration der IBD-Maschinen verantwortlich ist.

PIN (persönliche Identifizierungsnummer)

[0755] Personal Identification Number: Verfahren zur Einschränkung des Zugriffs auf das Konto eines Individuums auf der Basis von Geheimwissen; bestehend aus zumindest einer Nummer.

PIC (persönlicher Identifizierungscode)

[0756] Personal Identification Code: PIN bestehend aus Nummern, Symbolen oder alphabetischen Zeichen.

POS (Kasse)

[0757] Point of Sale: Ort, an dem Produkte verkauft werden.

PPT (Kassen-Telefonendgerät)

[0758] Phone Point-of-Sale Terminal: kombiniert Telefonnummer mit Händlerpreis und Produktinformation, um eine Transaktion über ein mit BIA ausgestattetes Telefon zu autorisieren. Bestellung/Autorisierung/Zustelladresse/PO weitergeleitet an Händler. Die resultierende Autorisierung wird gemeinsam mit dem privaten Code des Individuums auf der Telefon-LCD angezeigt oder „ausgesprochen".

RAM (Direktzugriffsspeicher)

Random Access Memory

RF (Hochfrequenz)

[0759] Radio Frequency: bezieht sich im Allgemeinen auf die während des normalen Betriebs elektrischer Geräte ausgesendete Hochfrequenzenergie.

Registers (Register)

[0760] Für einen bestimmten Zweck vorgesehener Speicher, auf Chips reservierte Daten und gespeicherte Operanden für Instruktionen.

Requests (Anfragen bzw. Aufforderungen)

[0761] Elektronische Anweisungen von der BIA an das DPC, damit dieses das Individuum identifiziert und dadurch den Befehl des Individuums ausführt, sofern die Identifizierung erfolgreich ist.

RMD (Fernhändler-Datenbank)

[0762] Remote Merchant Database: enthält alle Händler-Identifizierungscodes für Händlertelefon und Kabel-TV-Shops; indexiert nach Händleridentifizierung. Enthält auch Systemverschlüsselungscodes pro Händler.

RPT (Einzelhandelskassen-Endgerät)

[0763] Retail Point-of-Sale Terminal: kombiniert codierte Informationen zur biometrischen Identität mit Informationen über Einzelhandelstransaktionen (möglicherweise ausgehend von einer elektronischen Kassa) und formuliert Autorisierungsaufforderungen des Systems über X.25-Netzwerke, Modems usw.

Secure Transmission (sichere Übertragung)

[0764] Elektronische Nachricht oder Faxnachricht, in deren Rahmen zumindest ein Teilnehmer von DPC identifiziert wurde.

SFT (Endgerät für sichere Faxnachrichten)

[0765] Secured Fax Terminal: bedient sich der BIA, um Absender zu identifizieren, sendet Faxe entweder ungesichert, Absender-gesichert, gesichert oder gesichert-vertraulich Die letzteren beiden Typen erfordern es, dass sich die Empfänger mittels Biometrik-PIN identifizieren. Verwendet „Titel" (angegeben mit einer Titelindexziffer), um abgehende Faxe zu markieren. Der Absender möchte sich möglicherweise über den Zustellstatus informieren. Beide Teilnehmer müssen Systemmitglieder sein. Entweder der Absender oder der Empfänger können die Archivierung des Faxes anfordern.

SNM (Folgenummermodul)

[0766] Sequence Number Module: Softwaremodul im DPC, das für die DUKPT-Folgenummerverarbeitung für eingehende Anfragepakete verantwortlich ist. Die Folgenummerverarbeitung ist ein Schutz vor Wiedergabeangriffen.

Terminal (Endgerät)

[0767] Vorrichtung, die mit BIA ausgestattet ist, um biometrische Proben zu erfassen und Anfragenachrichten zu erstellen, die anschließend zwecks Autorisierung und Ausführung an das DPC übermittelt werden. Endgeräte fügen den Anfragenachrichten, identifizierenden Gegenteilnehmern u. dgl. fast immer Zusatzinformationen an.

Title Index Code (Titelindexcode)

[0768] Alphanumerische Folge, die die autorisierte Rolle oder Funktion eines Individuums in seinem beruflichen Umfeld eindeutig identifiziert.

Token

[0769] Unbelebtes Objekt, das eine Fähigkeit verleiht.

Tracking Code (Verfolgungscode)

[0770] Alphanumerische Folge, die Daten zugeordnet ist (im DPC gespeichert oder von diesem übermittelt), so dass man die Folge dazu verwenden kann, die Daten rückzurufen oder einen Bericht über den Daten-Übertragungsstatus zu erhalten.

Transaction (Transaktion)

Elektronischer Finanzaustausch

Transmission (Übertragung)

[0771] Elektronische Nachricht, die kein elektronischer Finanzaustausch ist.

VAD (Datenbank gültiger Vorrichtungen)

[0772] Valid Apparatus Database: zentrale Aufbewahrungsstelle, in der jede BIA (mit zugehörigen eindeutigen Verschlüsselungscodes) gemeinsam mit den BIA-Besitzern identifiziert ist.

Patentansprüche

1. Computersystem zur freiwilligen Identifizierung ohne Identitätsmarker, um die Identität eines Individuums aufgrund einer Überprüfung zumindest einer biometrischen Bid-Probe und eines persönlichen Bid-Identifizierungscodes, der während eines Bidschritts erfasst wurde, und des Vergleichs mit zuvor aufgezeichneten biometrischen Registrierungsproben und persönlichen Registrierungsidentifizierungscodes zu bestimmen, die während eines Registrierungsschritts erfasst wurden, wobei das System umfasst:
a. zumindest einen Computer;
b. erste Erfassungsmittel zum freiwilligen Eintragen zumindest einer biometrischen Registrierungsprobe und eines persönlichen Registrierungsidentifizierungscodes von einem Individuum während des Registrierungsschritts;
c. zweite Erfassungsmittel zum freiwilligen Eintragen zumindest einer biometrischen Bid-Probe und eines persönlichen Bid-Identifizierungscodes von einem Individuum während des Bid-Schritts;
d. erste Zusammenschaltungsmittel, um das erste und das zweite Erfassungsmittel mit dem Computer zusammenzuschalten, um die erfassten biometrischen Proben- und persönlichen Identifizierungscodes vom ersten und vom zweiten Erfassungsmittel zum Computer zu übertragen;
e. Mittel zum Speichern einer Vielzahl biometrischer Registrierungsproben;
f. Mittel zum Zuordnen eines Teilsatzes der gespeicherten biometrischen Registrierungsproben zu einem persönlichen Registrierungsidentifizierungscode;
g. Mittel zum Vergleichen einer biometrischen Bid-Probe mit den biometrischen Registrierungsproben, die dem persönlichen Registrierungsidentifizierungscode zugeordnet sind, der dem persönlichen Bid-Identifizierungscode entspricht, um eine Bewertung zu ergeben;
h. Ausführungsmittel innerhalb des Computers zur Speicherung von Daten und Verarbeitung und Ausführung von Befehlen, um eine Bestimmung zu erhalten; und
i. Mittel zum Ausgeben der Bewertung oder Bestimmung aus dem Computer.

2. Vorrichtung nach Anspruch 1, wobei das erste und das zweite Erfassungs- und Anzeigenmittel weiters umfassen:
a. zumindest ein biometrisches Eingabemittel zum Erfassen biometrischer Proben, das weiters eine Hardware- und eine Software-Komponente umfasst;
b. zumindest ein Endgerätmittel, das funktionell teilweise oder vollständig mit dem biometrischen Eingabemittel integriert ist, um zusätzliche Daten einzutragen und anzufügen;
c. zumindest ein Dateneintragungsmittel zum Eintragen eines persönlichen Identifizierungscodes, worin das Mittel entweder mit dem biometrischen Eingabemittel oder dem Endgerätmittel integriert ist; und
d. zweite Zusammenschaltungsmittel zum Zusammenschalten des biometrischen Eingabemittels, des Dateneintragungsmittels und des Endgeräts.

3. Vorrichtung nach Anspruch 2, worin das biometrische Eingabemittel einen Hardware-Identifizierungscode aufweist, der zuvor im Computer registriert worden ist, was das biometrische Eingabemittel für den Computer eindeutig identifizierbar macht.

4. Vorrichtung nach Anspruch 2, worin die Hardware-Komponente weiters umfasst:
a. zumindest ein Berechnungsmodul zur Datenverarbeitung;
b. löschbare und nicht löschbare Speichermodule zur Speicherung von Daten und Software;
c. eine biometrische Abtastvorrichtung zur Eingabe von Biometrik-Daten;
d. Dateneintragungsmittel zum Eintragen von Daten;
e. einen digitalen Übertragungsanschluss; und
f. Mittel zur Verhinderung von elektronischem Abhören.

5. Vorrichtung nach Anspruch 2, worin die Hardware-Komponente weiters ein drahtloses Übertragungsmittel umfasst.

6. Vorrichtung nach Anspruch 2, worin sich eine Software-Komponente in einem Berechnungsmodul befindet und weiters umfasst:
a. ein elektronisch löschbares Speichermodul, worin zumindest ein Befehlschnittstellenmodul, ein erster Satz aus Software und zugeordneten Daten gespeichert sind, die spezifisch für die beabsichtigte Verwendung der biometrischen Eingabevorrichtung und Daten konfiguriert sind; sowie
b. ein nicht löschbares Speichermodul, worin ein zweiter Satz aus Software und verknüpften Daten gespeichert sind.

7. Vorrichtung nach einem der Ansprüche 2 bis 6, in der eine Software-Komponente weiters Mittel zum Verschlüsseln von Daten aus Klartext in verschlüsselten Text umfasst.

8. Vorrichtung nach Anspruch 2, worin das Endgerät aus der aus Faxgeräten, Telefonen, TV-Fernbedienungen, PCs, Kredit/Kontokarten-Prozessor, Registrierkassen, Geldausgabeautomaten und drahtlosen PCs bestehenden Gruppe ausgewählt ist.

9. Vorrichtung nach Anspruch 1, worin das Vergleichsmittel weiters Mittel zum Identifizieren der biometrischen Eingabevorrichtung umfasst.

10. Vorrichtung nach Anspruch 1, worin die Computersysteme weiters umfassen:
a. zumindest ein Gegenteilnehmer-Computersystem; und
b. dritte Zusammenschaltungsmittel, um die Computersysteme mit dem Gegenteilnehmer-Computersystem zusammenzuschalten.

11. Vorrichtung nach Anspruch 1, worin die Datenbank weiters eine individuelle biometrische Datenbank umfasst.

12. Vorrichtung nach Anspruch 1, umfassend:
Mittel zum Vergleichen der von einem ersten Individuum entnommenen biometrischen Probe mit beliebigen zuvor gespeicherten biometrischen Proben im Teilsatz, der dem einen persönlichen Identifizierungscode zugeordnet ist, um sicherzustellen, dass die vom ersten Individuum eingetragene biometrische Probe für jede zuvor gespeicherte biometrische Probe im gleichen Teilsatz, der von zumindest einem zweiten Individuum bereitgestellt wird, algorithmisch eindeutig ist; und
Mittel zum Speichern der eingetragenen biometrischen Probe vom ersten Individuum im ausgewählten persönlichen Identifizierungscode-Korb, wenn die Probe gegenüber jeder zuvor gespeicherten biometrischen Probe von dem zumindest einen zweiten Individuum algorithmisch eindeutig ist.

13. Verfahren zur Schnellsuche zumindest einer ersten zuvor gespeicherten biometrischen Probe von einem ersten Individuum unter Verwendung eines persönlichen Identifzierungscode-Korbs, der fähig ist, zumindest eine algorithmisch eindeutige zweite biometrische Probe von zumindest einem zweiten Individuum zu enthalten, und der der durch den persönlichen Identifizierungscode identifiziert ist, umfassend:
a. einen Speicherschritt, der weiters umfasst:
i. das Auswählen eines persönlichen identifizierungscodes durch ein erstes Individuum;
ii. das Eintragen einer biometrischen Probe vom ersten Individuum;
iii. das Lokalisieren des persönlichen Identifizierungscode-Korbs, der durch den persönlichen Identifizierungscode identifiziert ist, der vom ersten Individuum ausgewählt wurde;

iv. das Vergleichen der vom ersten Individuum genommenen biometrischen Probe mit zuvor gespeicherten biometrischen Proben im ausgewählten persönlichen Identifizierungscode-Korb, um sicherzustellen, dass die vom ersten Individuum eingetragene biometrische Probe gegenüber der zuvor gespeicherten, zumindest einen biometrischen Probe, die vom zumindest einen zweiten Individuum bereitgestellt wurde, algorithmisch eindeutig ist; und
v. das Speichern der eingetragenen biometrischen Probe vom ersten Individuum im ausgewählten persönlichen Identifizierungscode-Korb, wenn die Probe gegenüber zumindest einer zuvor gespeicherten biometrischen Probe vom zumindest einen zweiten Individuum algorithmisch eindeutig ist; und
b. einen Bid-Schritt, der weiters umfasst:
i. das Eintragen des ausgewählten persönlichen Identifizierungscodes durch das erste Individuum; und
ii. das Eintragen einer biometrischen Probe durch das erste Individuum; sowie
c. einen Vergleichsschritt, der weiters umfasst:
i. das Finden des persönlichen Identifizierungscode-Korbs, der durch den persönlichen Identifizierungscode identifiziert wird, der vom ersten Individuum eingetragen wird; und
ii. das Vergleichen der eingetragenen biometrischen Probe vom ersten Individuum mit der zumindest einen gespeicherten biometrischen Probe vom zumindest einen zweiten Individuum im eingetragenen persönlichen Identifizierungscode-Korb, um entweder ein erfolgreiches oder ein erfolgloses Identifizierungsergebnis zu erzeugen.

14. Verfahren nach Anspruch 13, worin der Speicherschritt weiters die Wahl eines privaten Codes durch das erste Individuum umfasst.

15. Verfahren nach Anspruch 14, worin das Verfahren weiters einen Ausführungsschritt umfasst, worin ein Befehl verarbeitet und ausgeführt wird, um eine Bestimmung zu ergeben.

16. Verfahren nach Anspruch 14 oder 15, worin das Verfahren weiters einen Ausgabeschritt umfasst, worin das Identifizierungsergebnis oder die Bestimmung nach außen gebracht und angezeigt wird.

17. Verfahren nach einem der Ansprüche 14 bis 16, worin das Verfahren weiters einen Präsentationsschritt umfasst, worin bei der erfolgreichen Identifizierung des ersten Individuums dem ersten Individuum der private Code präsentiert wird.

18. Verfahren nach Anspruch 13, worin sowohl der Registrierungs- als auch der Bid-Schritt weiters einen Datenversiegelungsschritt umfassen, um die Fähigkeit zu bieten, eine Veränderung der Daten zu detektieren, weiters umfassend:
a. einen Geheimschlüssel; und
b. eine irreversible Einweg-Transformation der Daten, die ohne den Geheimschlüssel nicht reproduziert werden kann.

19. Verfahren nach Anspruch 15, worin der Ausführungsschritt des Verfahrens die Ausführung einer elektronischen Finanztransaktion umfasst.

Es folgen 20 Blatt Zeichnungen

Anhängende Zeichnungen

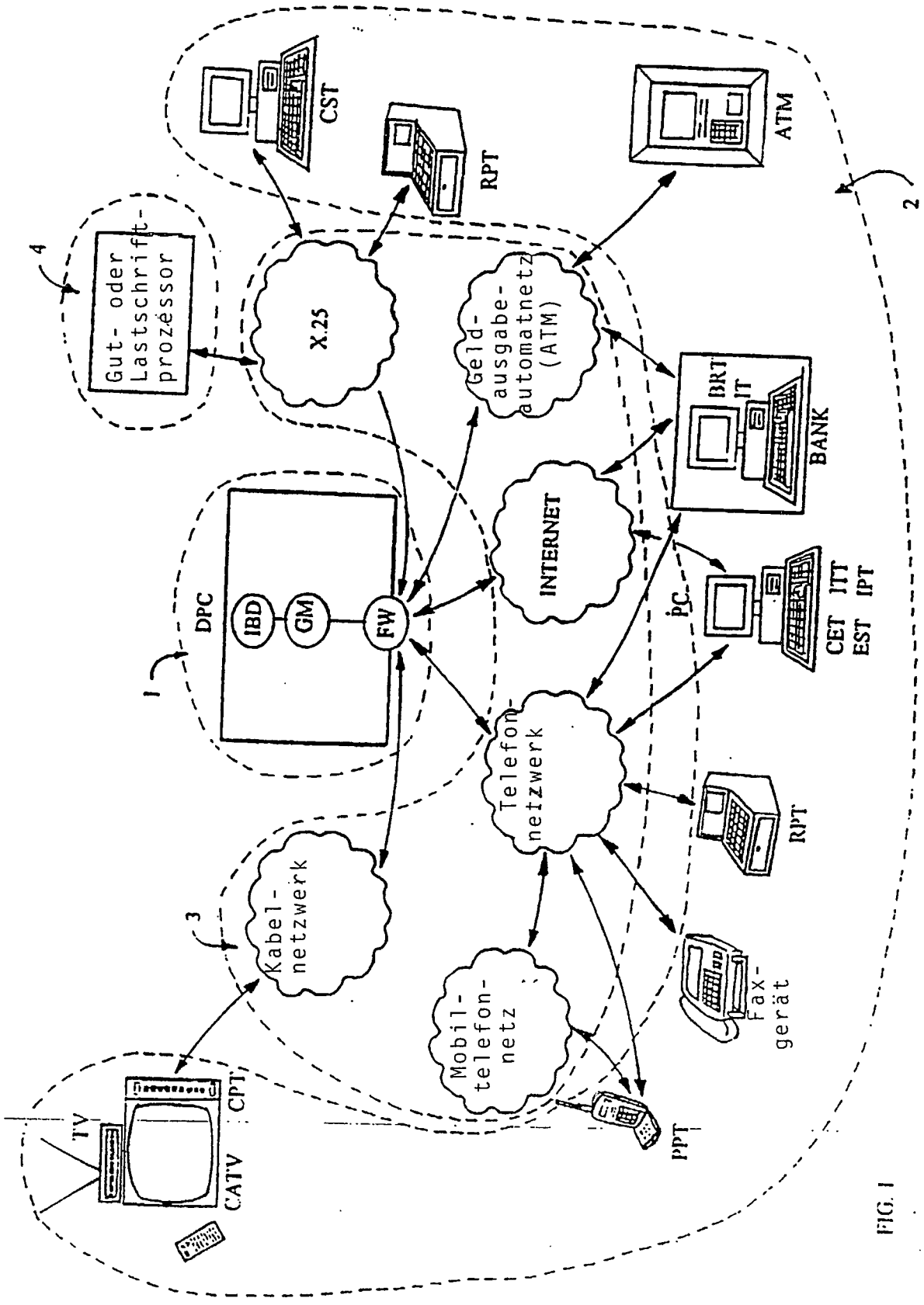

FIG. 1

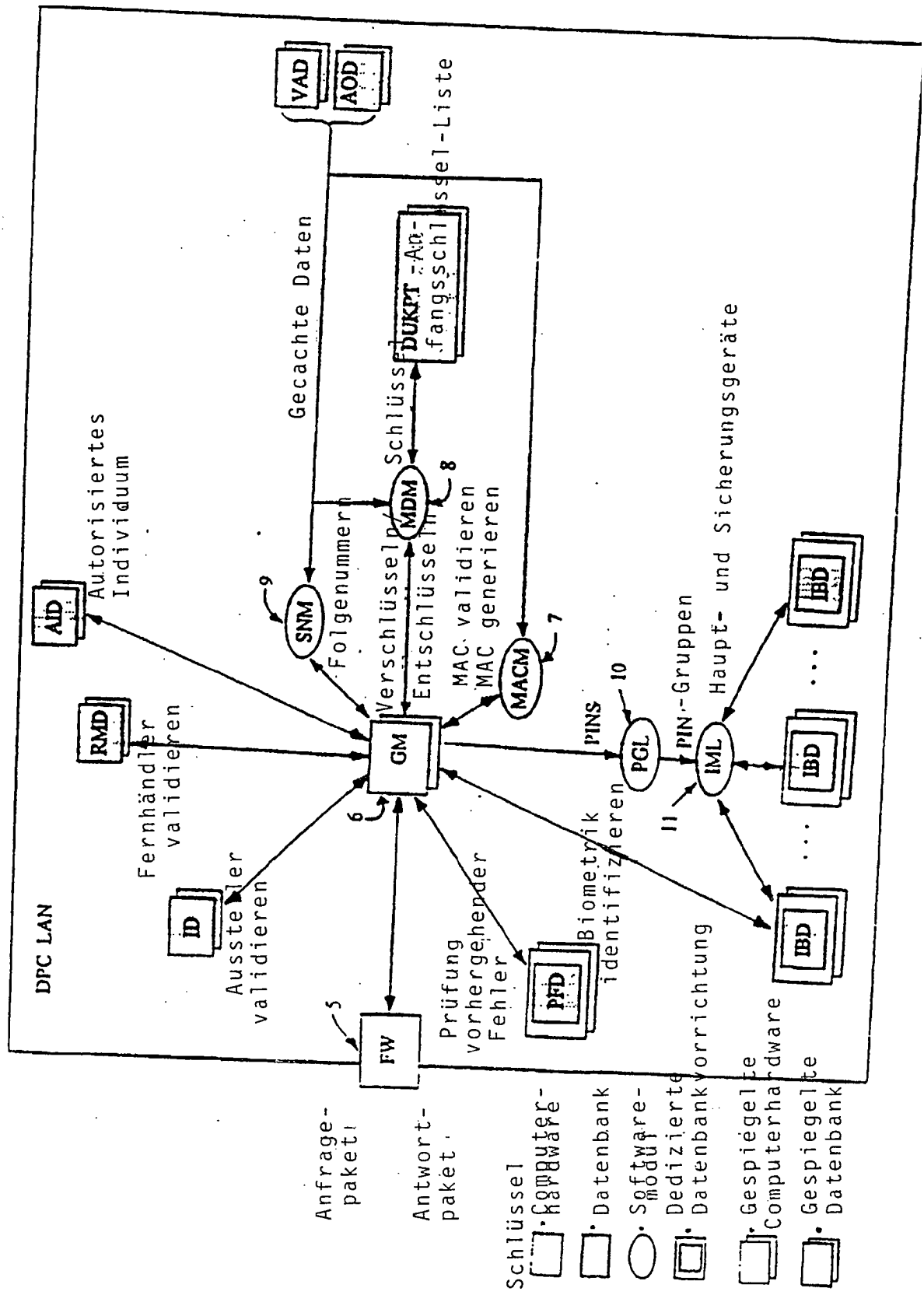
DPC LAN
AID
Autorisiertes Individuum
RMD
Fernhändler validieren
ID
Aussteller validieren
FW
5
GM
6
SNM
9
Folgenummern
Verschlüsseln
MDM
8
Entschlüsseln
DUKPT - Anfangsschlüssel
Schlüssel
VAD
AOD
Gecachte Daten
Schlüssel-Liste
MACM
7
MAC validieren
MAC generieren
PINS
10
PGL
PIN-Gruppen
IML
Haupt- und Sicherungsgeräte
IBD
PFD
Prüfung vorhergehender Fehler
Biometrik identifizieren
11
Anfrage-paket
Antwort-paket
Schlüssel
Computer-hardware
Datenbank
Software-modul
Dedizierte Datenbankvorrichtung
Gespiegelte Computerhardware
Gespiegelte Datenbank

FIG. 2

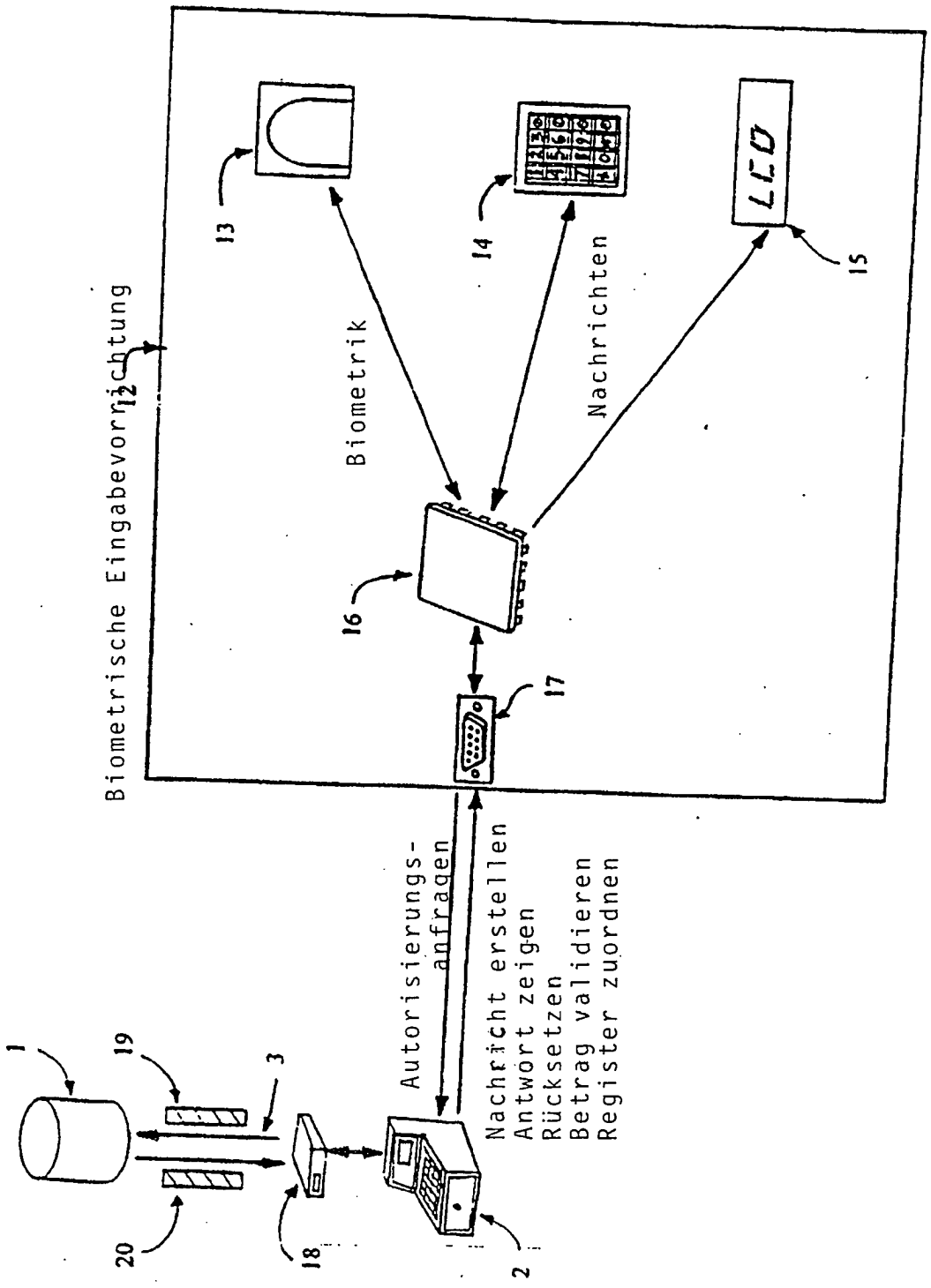
Biometrische Eingabevorrichtung
12
13
14
15
16
17
Biometrik
Nachrichten
LCD
Autorisierungs-anfragen
Nachricht erstellen
Antwort zeigen
Rücksetzen
Betrag validieren
Register zuordnen
1
19
3
20
18
2

FIG. 3

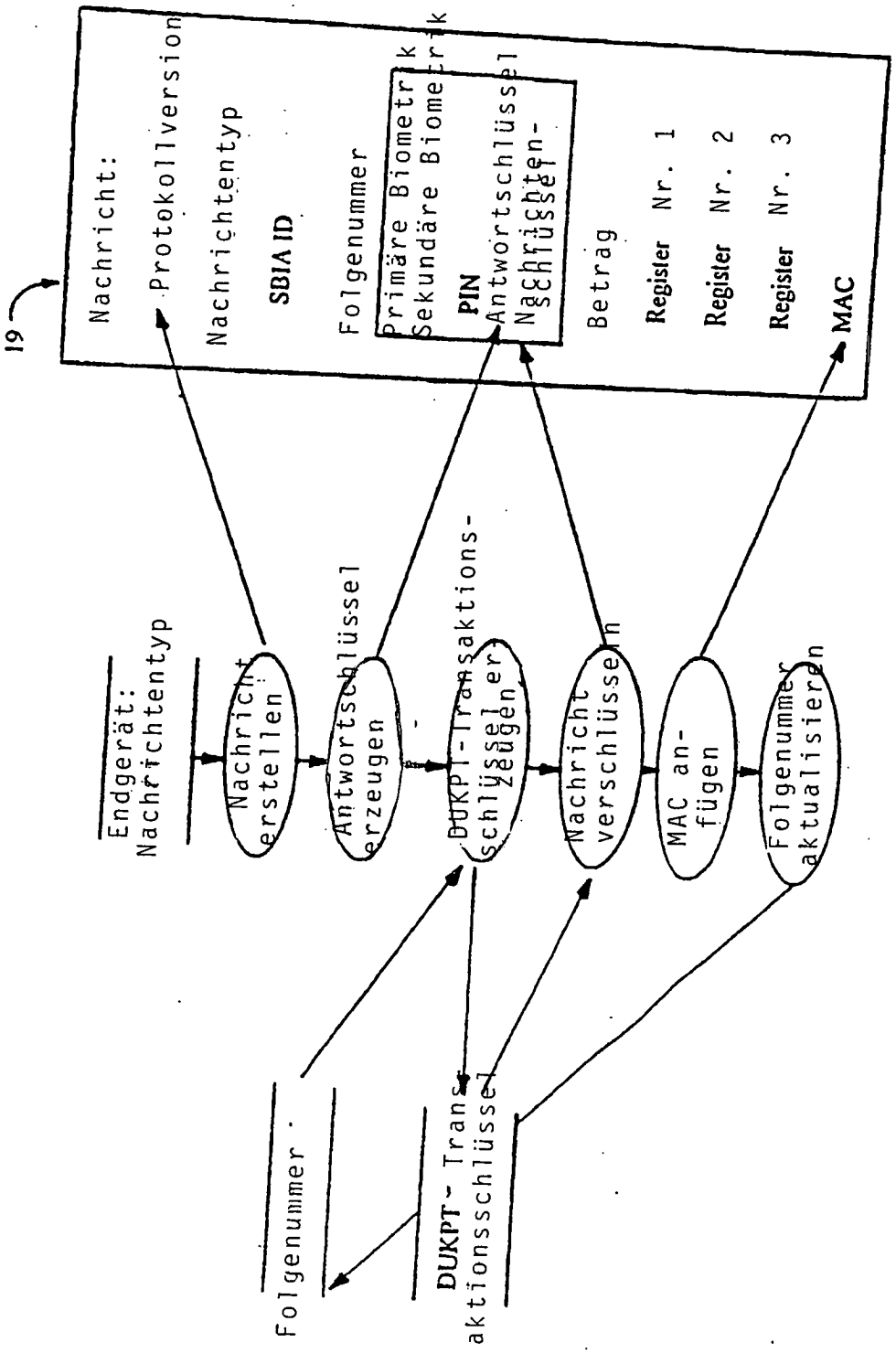
19
Nachricht:
Protokollversion
Nachrichtentyp
SBIA ID
Folgenummer
Primäre Biometrik
Sekundäre Biometrik
PIN
Antwortschlüssel
Nachrichten-
Betrag
Register Nr. 1
Register Nr. 2
Register Nr. 3
MAC
Endgerät:
Nachrichtentyp
Nachricht erstellen
Antwortschlüssel erzeugen
DUKPT-Transaktions-schlüssel erzeugen
Nachricht verschlüsseln
MAC an-fügen
Folgenummer aktualisieren
Folgenummer
DUKPT-Transaktionsschlüssel

FIG. 4

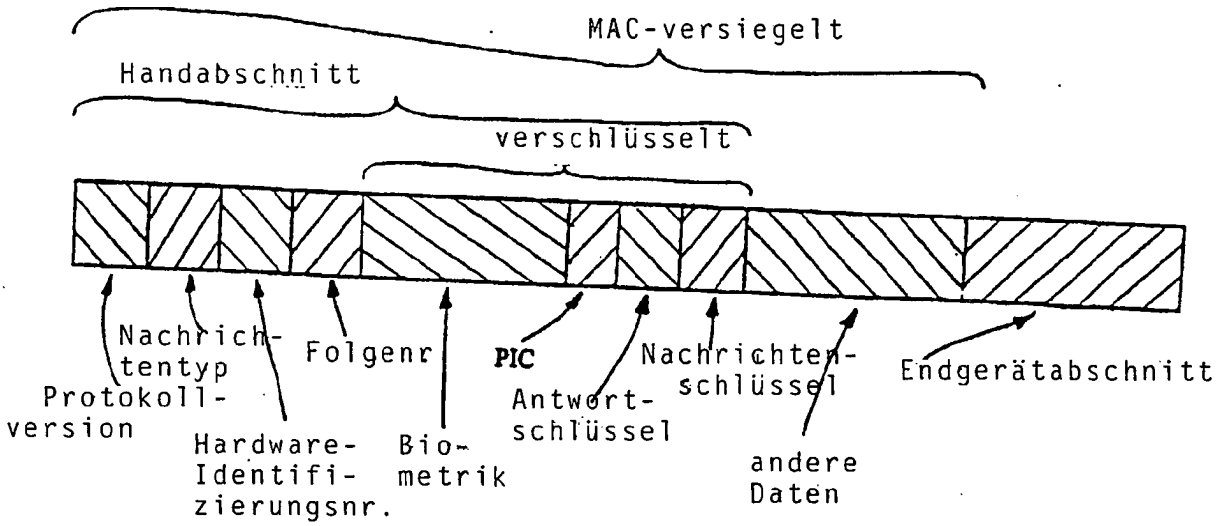
MAC-versiegelt
Handabschnitt
verschlüsselt
Nachrich-
tentyp
Folgenr
PIC
Nachrichten-
schlüssel
Endgerätabschnitt
Protokoll-
version
Antwort-
schlüssel
Hardware-
Identifi-
zierungsnr.
Bio-
metrik
andere
Daten

FIG. 5

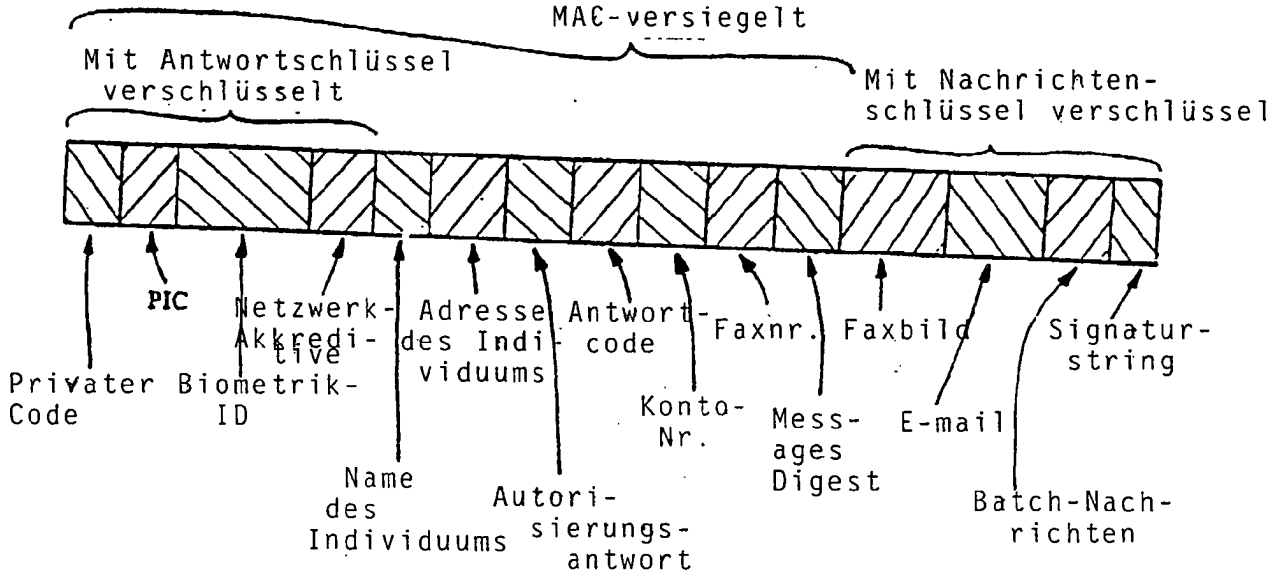
MAC-versiegelt
Mit Antwortschlüssel
verschlüsselt
Mit Nachrichten-
schlüssel verschlüssel
PIC
Netzwerk-
Akkredi-
tive
Adresse
des Indi-
viduums
Antwort-
code
Faxnr.
Faxbild
Signatur-
string
Privater
Code
Biometrik-
ID
Konto-
Nr.
Mess-
ages
Digest
E-mail
Name
des
Individuums
Autori-
sierungs-
antwort
Batch-Nach-
richten

FIG. 6

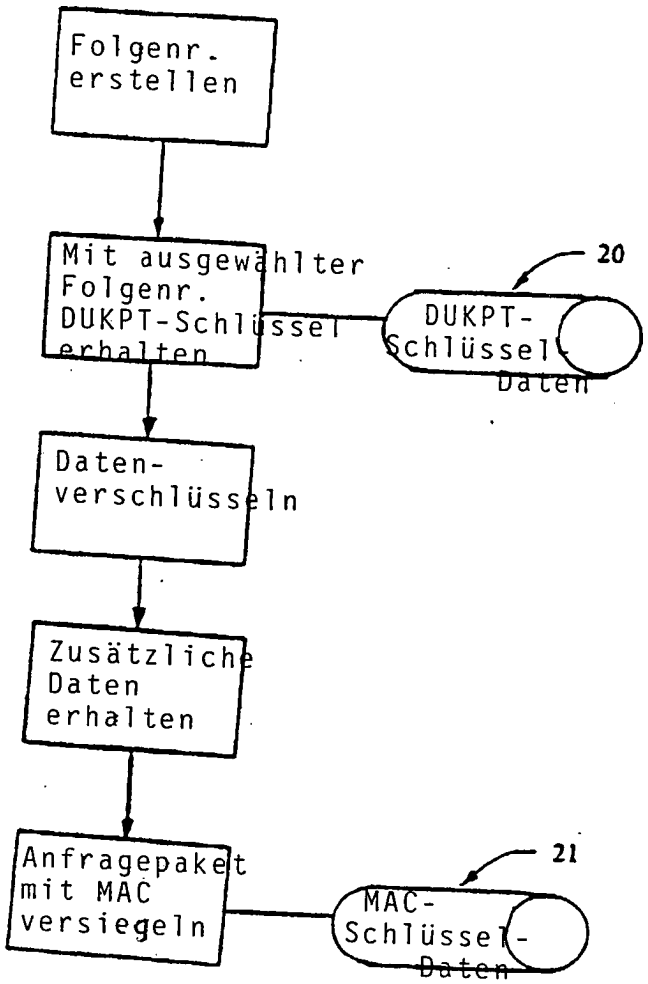
Folgenr. erstellen
Mit ausgewählter Folgenr. DUKPT-Schlüssel erhalten
20
DUKPT-Schlüssel-Daten
Daten-verschlüsseln
Zusätzliche Daten erhalten
Anfragepaket mit MAC versiegeln
21
MAC-Schlüssel-Daten

FIG. 7

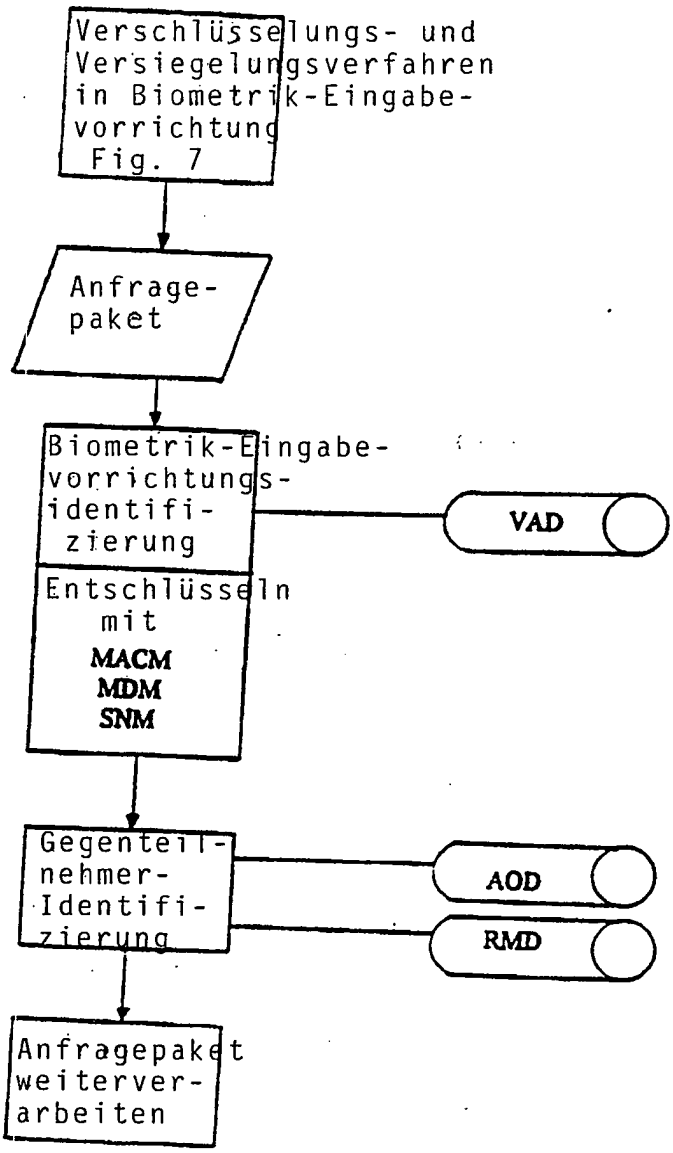
Verschlüsselungs- und Versiegelungsverfahren in Biometrik-Eingabe-vorrichtung Fig. 7
Anfrage-paket
Biometrik-Eingabe-vorrichtungs-identifi-zierung
VAD
Entschlüsseln mit
MACM
MDM
SNM
Gegenteil-nehmer-Identifi-zierung
AOD
RMD
Anfragepaket weiterver-arbeiten

FIG. 8

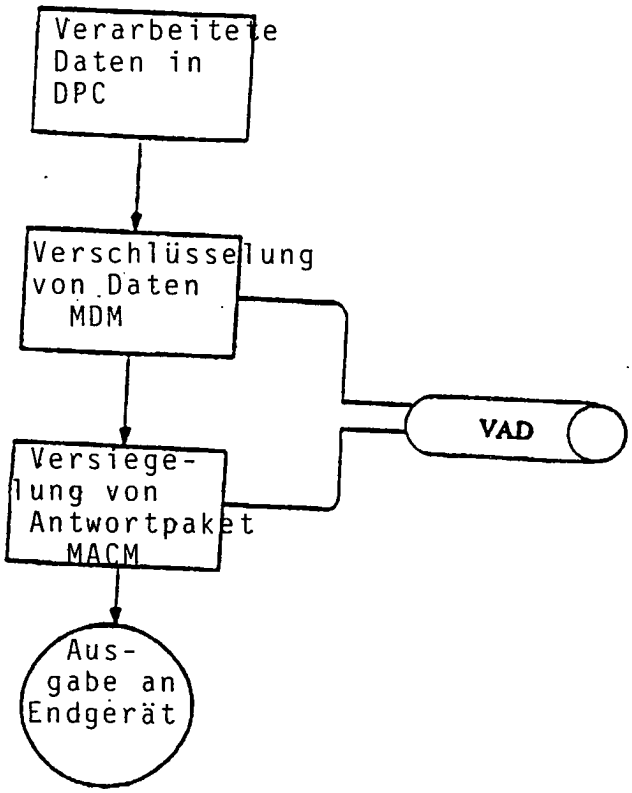
Verarbeitete Daten in DPC
Verschlüsselung von Daten MDM
VAD
Versiegelung von Antwortpaket MACM
Ausgabe an Endgerät

FIG. 9

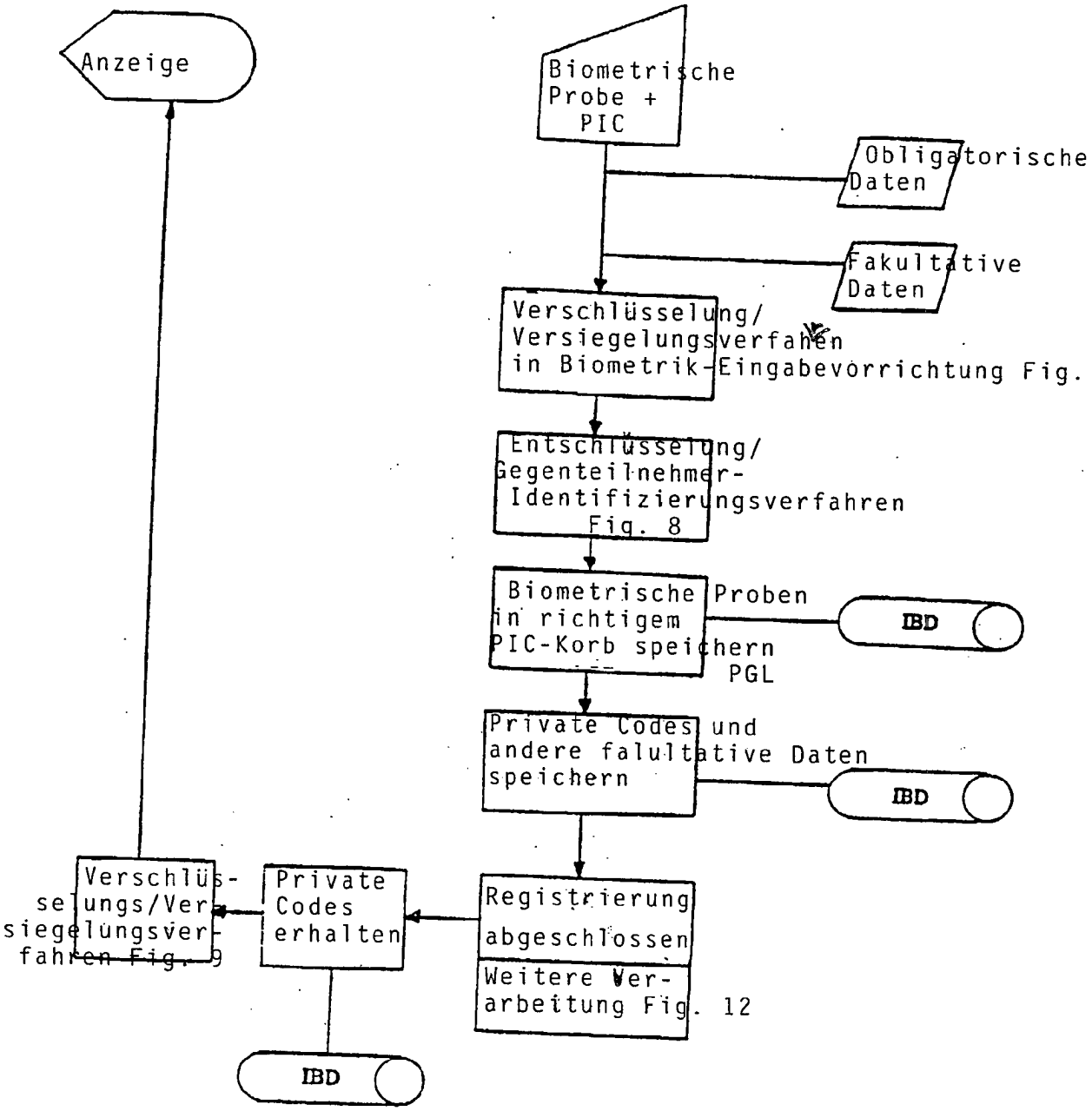
Anzeige
Biometrische Probe + PIC
Obligatorische Daten
Fakultative Daten
Verschlüsselung/ Versiegelungsverfahren in Biometrik-Eingabevorrichtung Fig.
Entschlüsselung/ Gegenteilnehmer-Identifizierungsverfahren Fig. 8
Biometrische Proben in richtigem PIC-Korb speichern
PGL
IBD
Private Codes und andere falultative Daten speichern
IBD
Registrierung abgeschlossen
Weitere Verarbeitung Fig. 12
Private Codes erhalten
Verschlüs-selungs/Ver-siegelungsver-fahren Fig. 9
IBD

FIG. 10

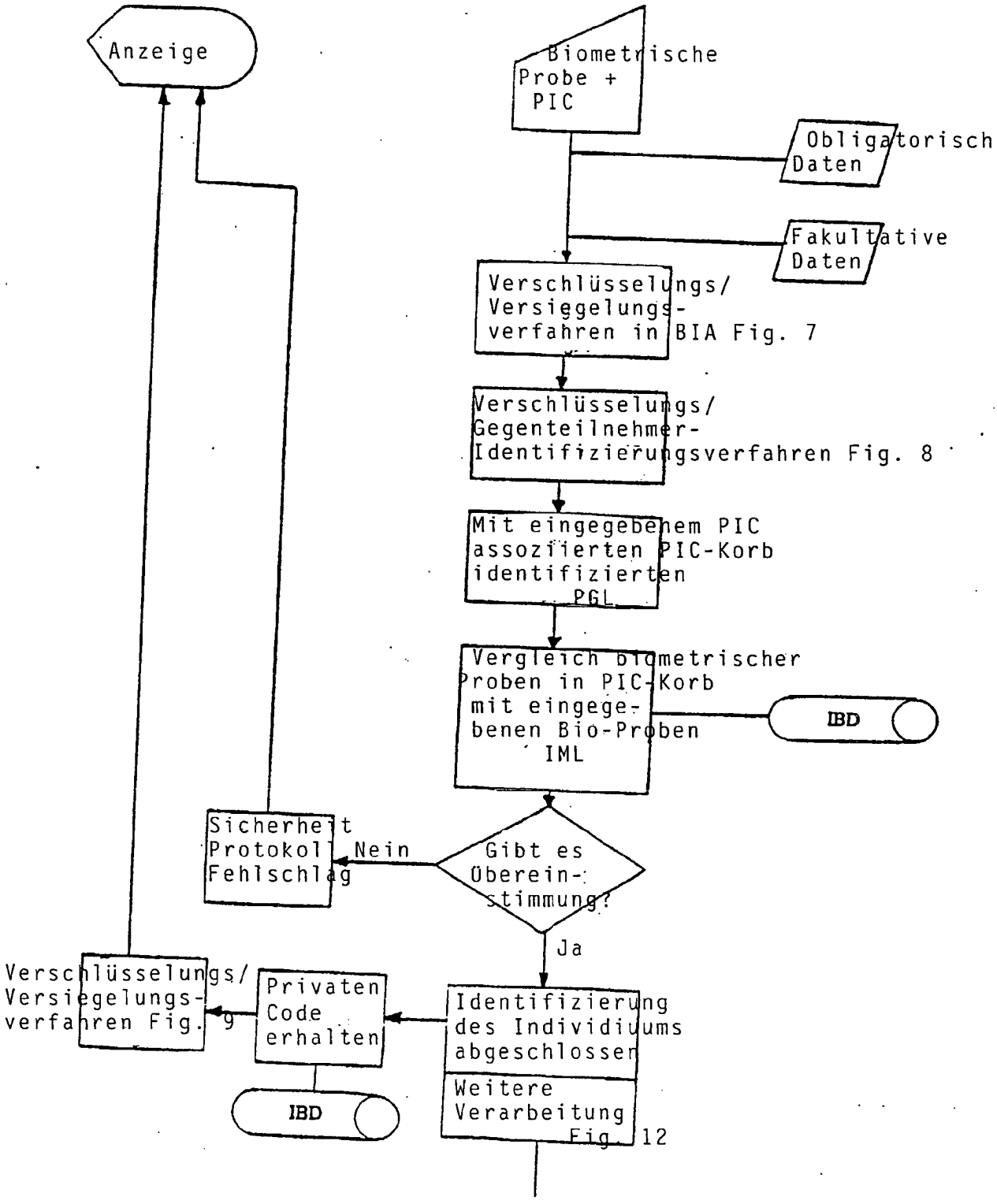
Anzeige
Biometrische Probe + PIC
Obligatorisch Daten
Fakultative Daten
Verschlüsselungs/ Versiegelungs- verfahren in BIA Fig. 7
Verschlüsselungs/ Gegenteilnehmer- Identifizierungsverfahren Fig. 8
Mit eingegebenem PIC assoziierten PIC-Korb identifizierten PGL
Vergleich biometrischer Proben in PIC-Korb mit eingege- benen Bio-Proben IML
IBD
Sicherheit Protokoll Fehlschlag
Nein
Gibt es Überein- stimmung?
Ja
Verschlüsselungs/ Versiegelungs- verfahren Fig. 9
Privaten Code erhalten
Identifizierung des Individiuums abgeschlossen
IBD
Weitere Verarbeitung Fig. 12

FIG. 11

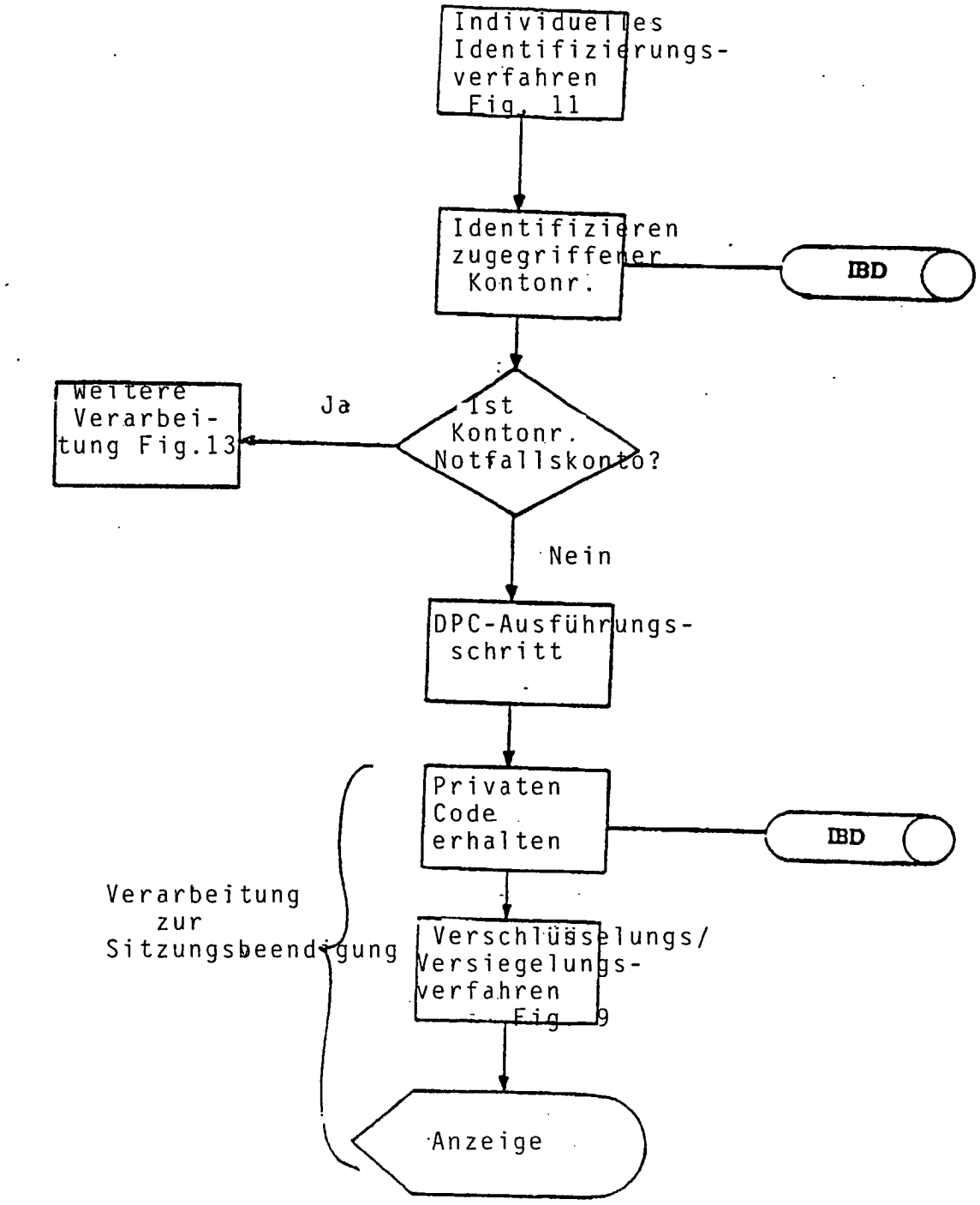
Individuelles Identifizierungs-verfahren Fig. 11
Identifizieren zugegriffener Kontonr.
IBD
Weitere Verarbeitung Fig.13
Ja
Ist Kontonr. Notfallskonto?
Nein
DPC-Ausführungs-schritt
Privaten Code erhalten
IBD
Verarbeitung zur Sitzungsbeendigung
Verschlüsselungs/ Versiegelungs-verfahren Fig. 9
Anzeige

FIG. 12

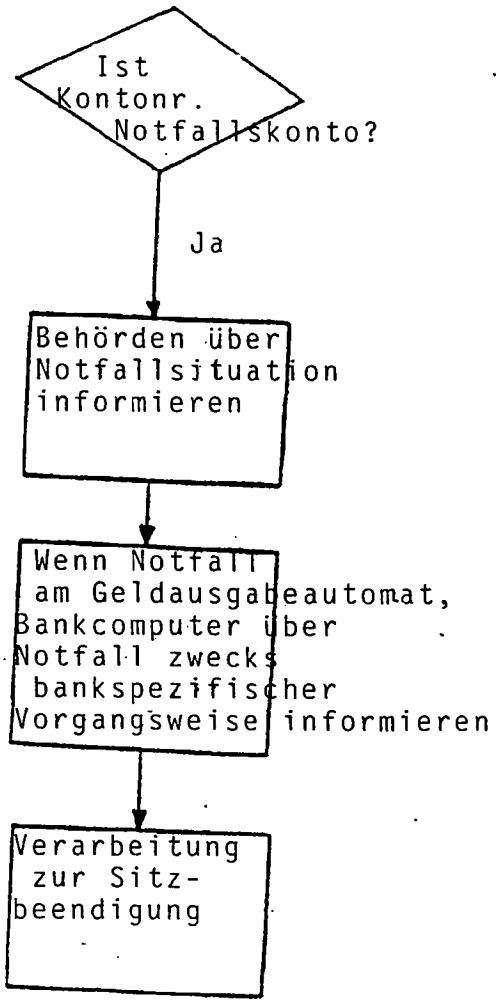
Ist Kontonr. Notfallskonto?
Ja
Behörden über Notfallsituation informieren
Wenn Notfall am Geldausgabeautomat, Bankcomputer über Notfall zwecks bankspezifischer Vorgangsweise informieren
Verarbeitung zur Sitz-beendigung

FIG. 13

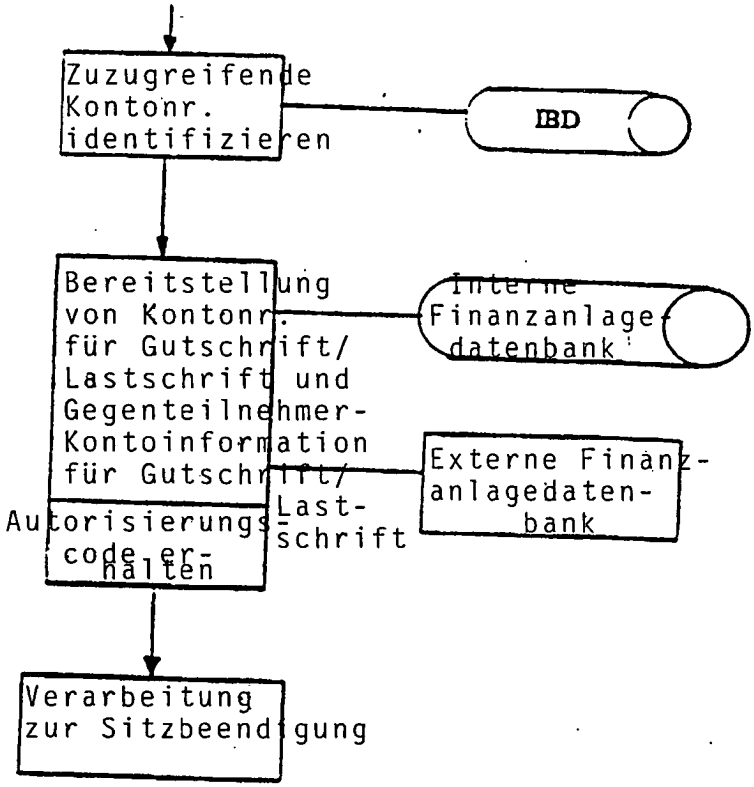
Zuzugreifende Kontonr. identifizieren
IBD
Bereitstellung von Kontonr. für Gutschrift/ Lastschrift und Gegenteilnehmer-Kontoinformation für Gutschrift/ Last-schrift
Interne Finanzanlage-datenbank
Externe Finanz-anlagedaten-bank
Autorisierungs-code er-halten
Verarbeitung zur Sitzbeendigung

FIG. 14

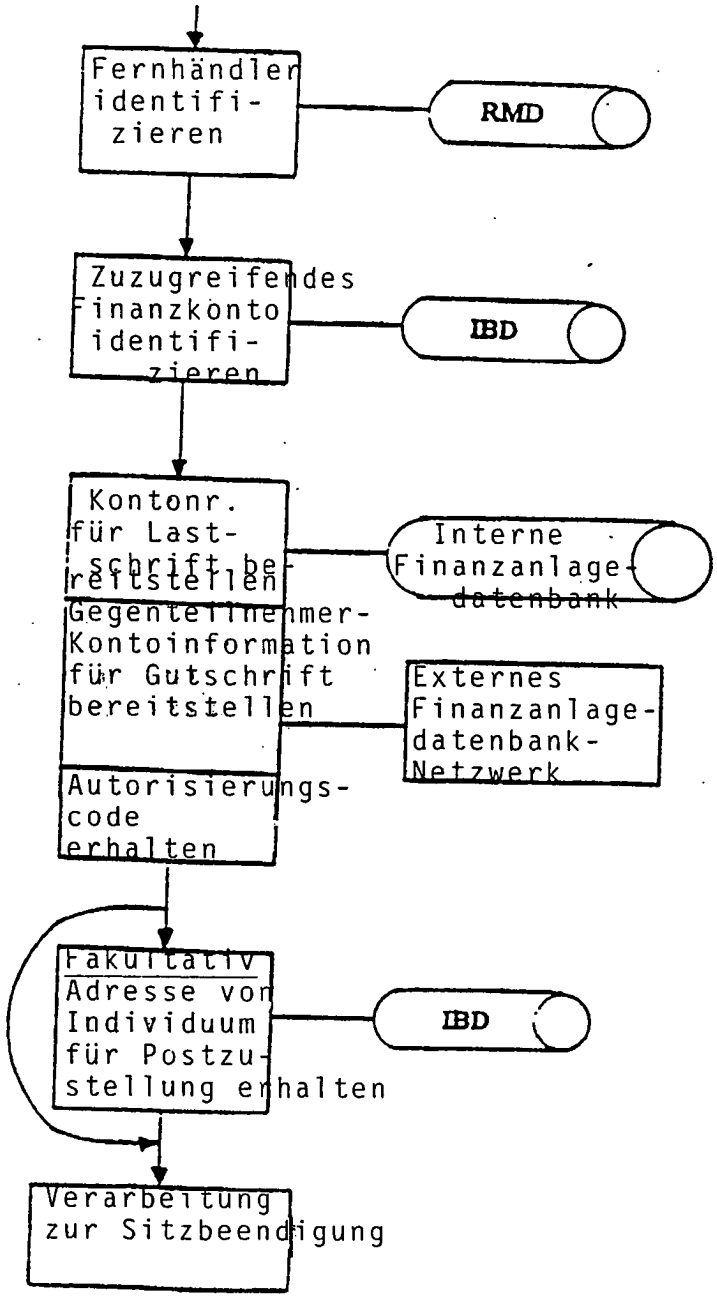
Fernhändler identifizieren
RMD
Zuzugreifendes Finanzkonto identifizieren
IBD
Kontonr. für Lastschrift bereitstellen
Interne Finanzanlage-datenbank
Gegenteilnehmer-Kontoinformation für Gutschrift bereitstellen
Externes Finanzanlage-datenbank-Netzwerk
Autorisierungscode erhalten
Fakultativ
Adresse von Individuum für Postzustellung erhalten
IBD
Verarbeitung zur Sitzbeendigung

FIG. 15

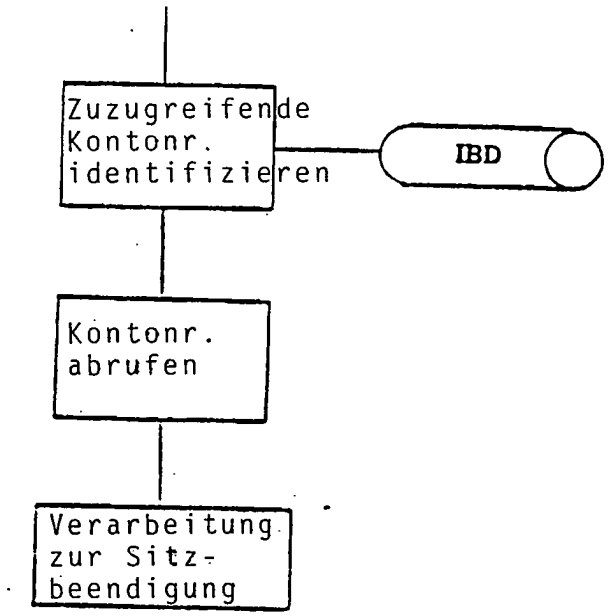
Zuzugreifende Kontonr. identifizieren
IBD
Kontonr. abrufen
Verarbeitung zur Sitz-beendigung

FIG. 16

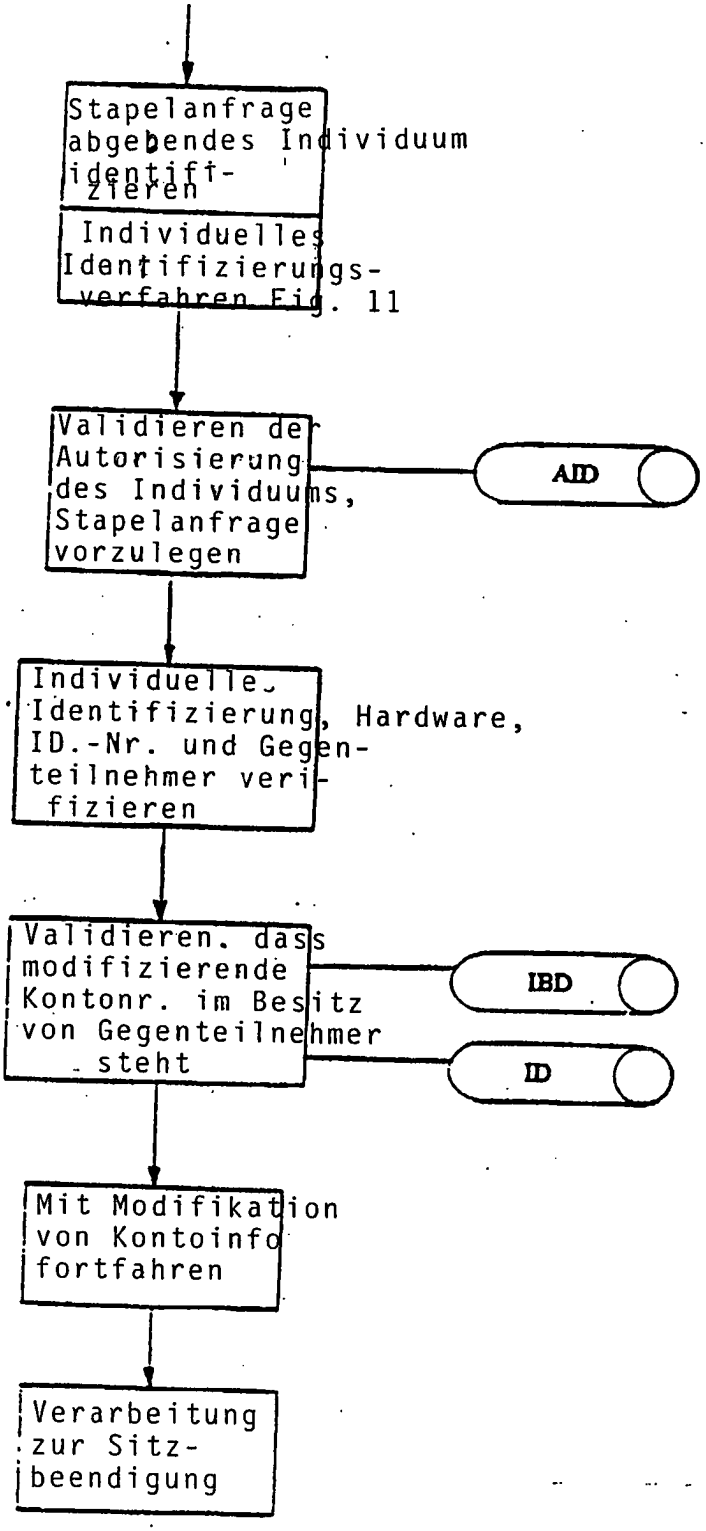
Stapelanfrage abgebendes Individuum identifizieren
Individuelles Identifizierungsverfahren Fig. 11
Validieren der Autorisierung des Individuums, Stapelanfrage vorzulegen
AID
Individuelle Identifizierung, Hardware, ID.-Nr. und Gegenteilnehmer verifizieren
Validieren, dass modifizierende Kontonr. im Besitz von Gegenteilnehmer steht
IBD
ID
Mit Modifikation von Kontoinfo fortfahren
Verarbeitung zur Sitzbeendigung

FIG. 17

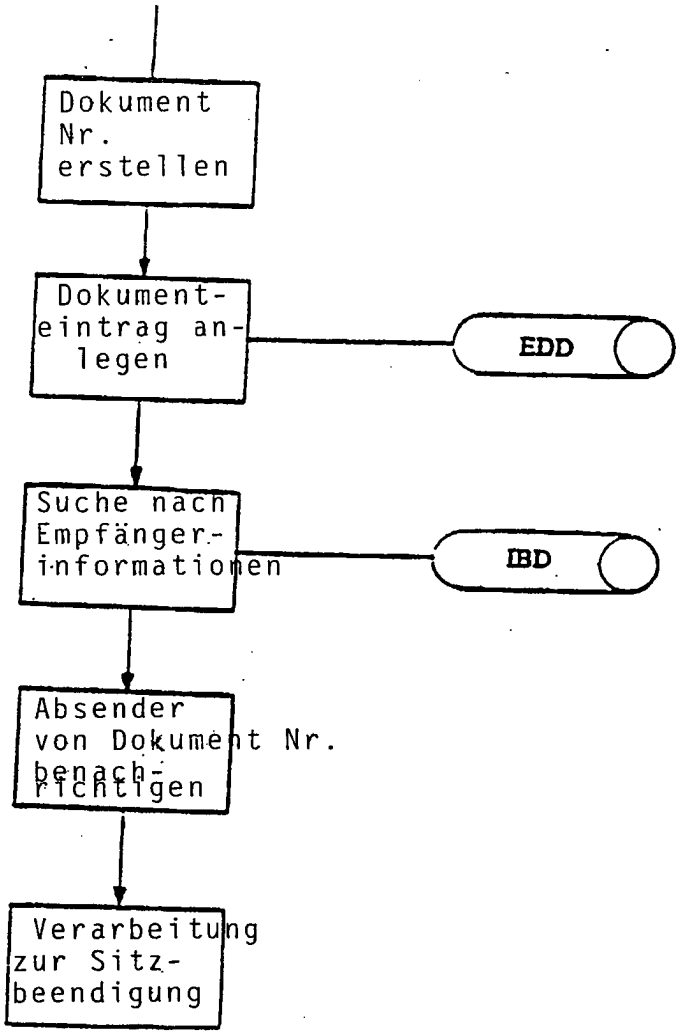
Dokument Nr. erstellen
Dokument-eintrag anlegen
EDD
Suche nach Empfänger-informationen
IBD
Absender von Dokument Nr. benachrichtigen
Verarbeitung zur Sitzbeendigung

FIG. 18

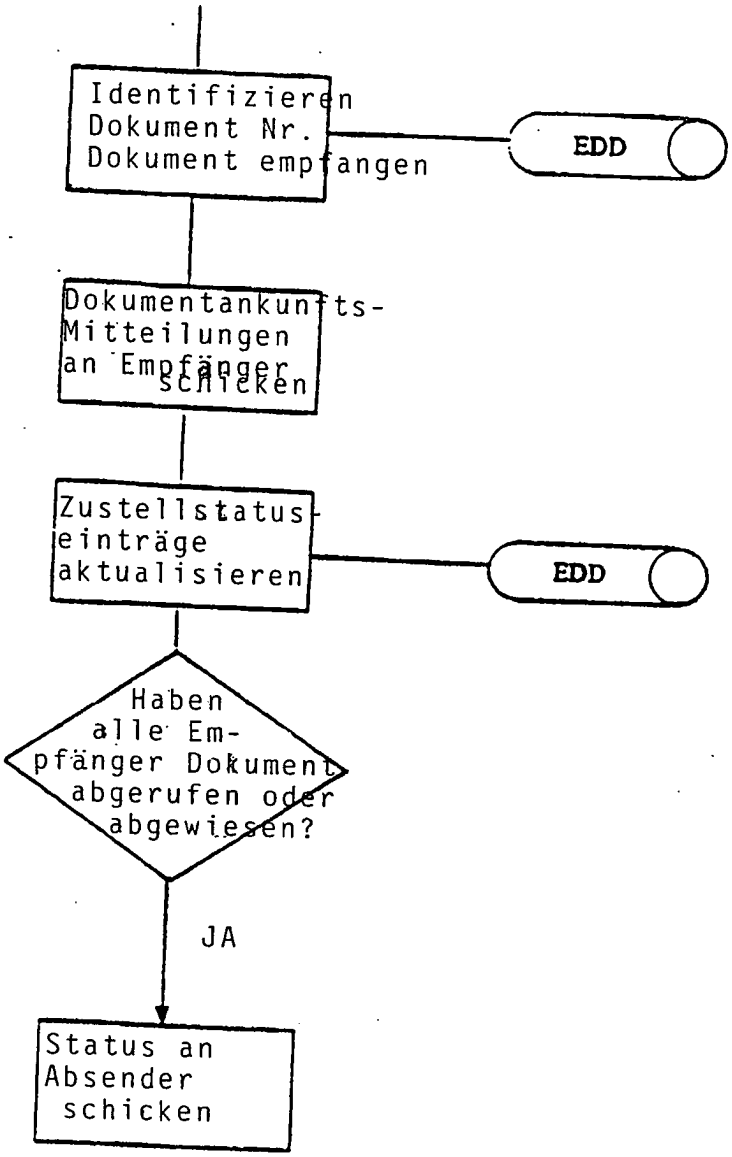
Identifizieren Dokument Nr. Dokument empfangen
EDD
Dokumentankunfts-Mitteilungen an Empfänger schicken
Zustellstatus-einträge aktualisieren
EDD
Haben alle Empfänger Dokument abgerufen oder abgewiesen?
JA
Status an Absender schicken

FIG. 19

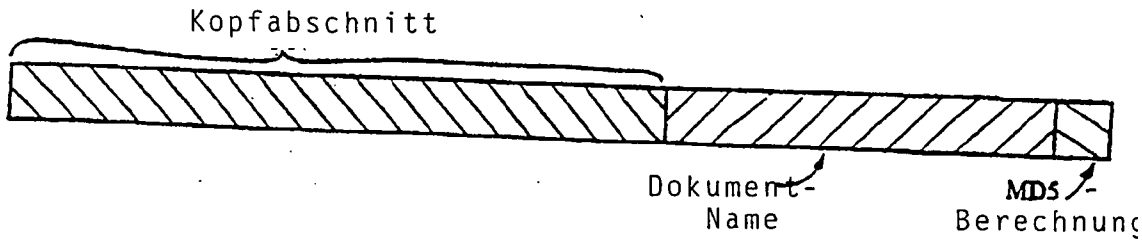

FIG. 20A

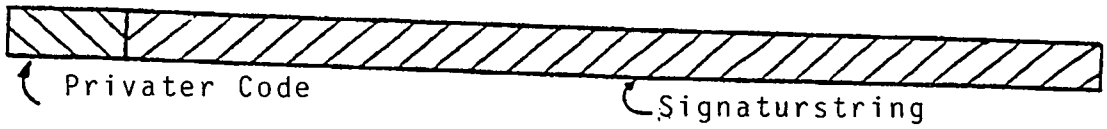

FIG. 20B

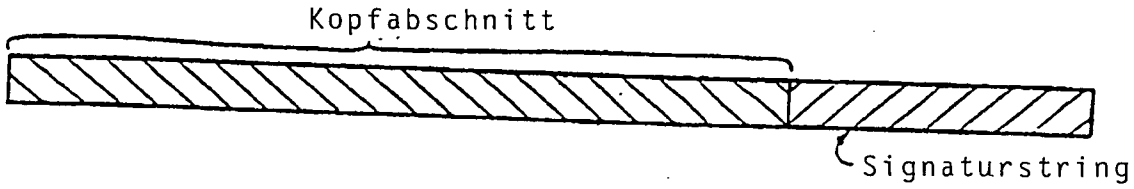

FIG. 20C

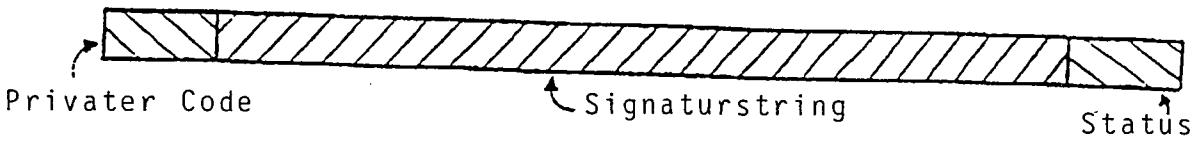

FIG. 20D

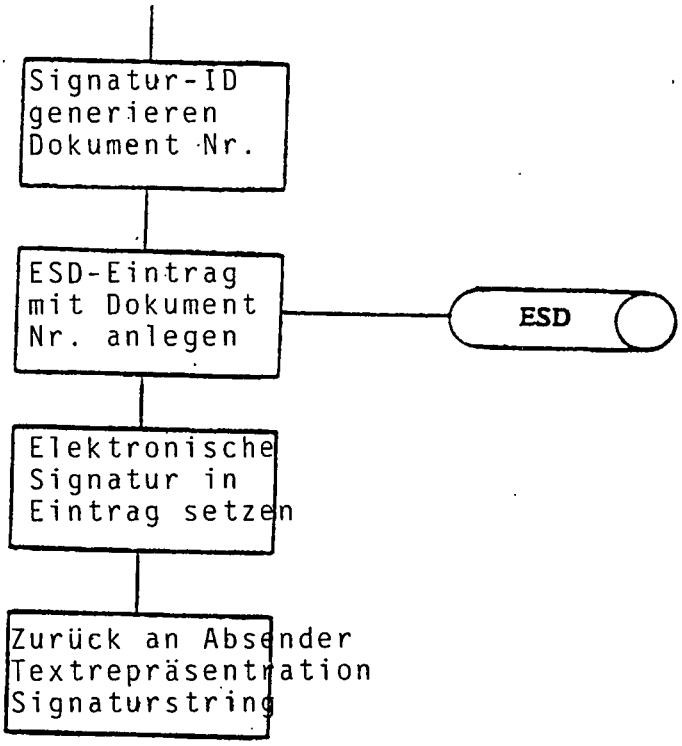
Signatur-ID generieren Dokument Nr.
ESD-Eintrag mit Dokument Nr. anlegen
ESD
Elektronische Signatur in Eintrag setzen
Zurück an Absender Textrepräsentation Signaturstring

FIG. 21

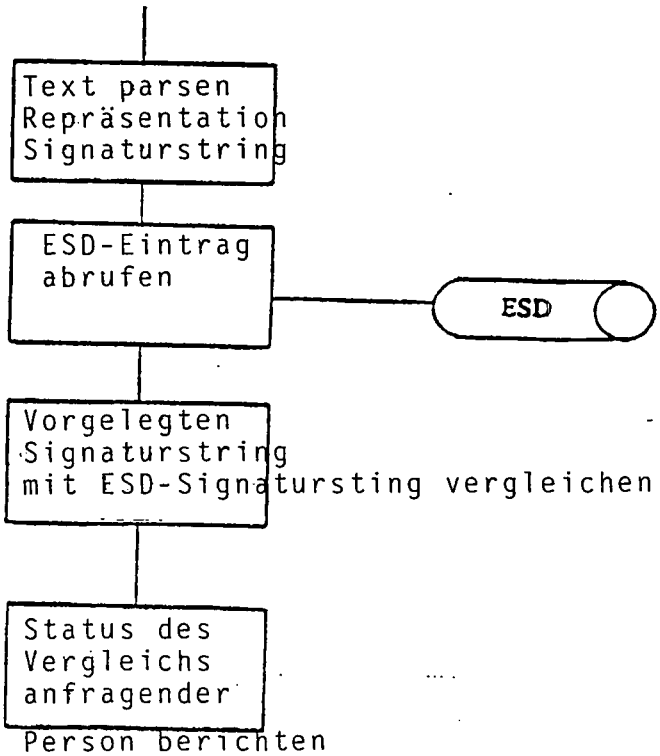
Text parsen Repräsentation Signaturstring
ESD-Eintrag abrufen
ESD
Vorgelegten Signaturstring mit ESD-Signatursting vergleichen
Status des Vergleichs anfragender Person berichten

FIG. 22