(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 103 93 215 T5** 2005.09.08

(12) **Veröffentlichung**

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2004/025545**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **103 93 215.1**
(86) PCT-Aktenzeichen: **PCT/US2003/028602**
(86) PCT-Anmeldetag: **10.09.2003**
(87) PCT-Veröffentlichungstag: **25.03.2004**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **08.09.2005**

(51) Int Cl.[7]: **G06K 9/00**

(30) Unionspriorität:

60/409,716	**10.09.2002**	**US**
60/409,715	**10.09.2002**	**US**
60/429,919	**27.11.2002**	**US**
60/433,254	**13.12.2002**	**US**
60/484,692	**03.07.2003**	**US**

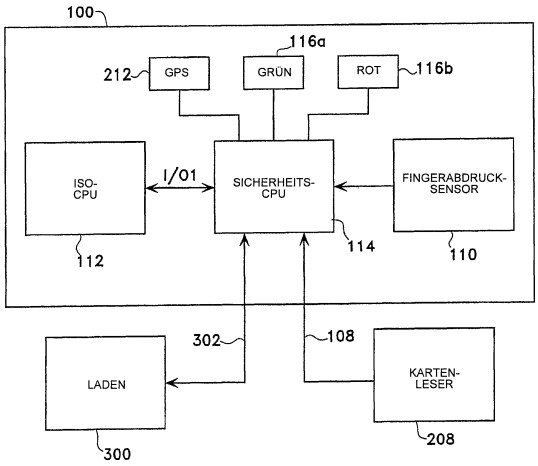
(71) Anmelder:
IVI Smart Technologies Inc., San Jose, Calif., US

(74) Vertreter:
Manitz, Finsterwald & Partner GbR, 80336 München

(72) Erfinder:
Saito, Tamio, San Francisco, Calif., US; Aida, Takashi, San Jose, Calif., US; Drizin, Wayne, San Jose, Calif., US

(54) Bezeichnung: **Sichere biometrische Identitätsverfikation**

(57) Hauptanspruch: Intelligente Identifikationskarte mit:
einem On-Board-Speicher zum Speichern von Referenzdaten,
einem On-Board-Sensor zum Nehmen originaler biometrischer Daten,
einem On-Board-Mikroprozessor zum Vergleich der genommenen biometrischen Daten mit entsprechenden gespeicherten Referenzdaten innerhalb einer vorbestimmten Schwelle und zum Erzeugen einer Verifikationsnachricht nur, wenn eine Übereinstimmung innerhalb einer vorbestimmten Schwelle vorhanden ist, und
einem Mittel zum Kommunizieren der Verifikationsnachricht an ein externes Netzwerk.



Beschreibung

QUERVERWEIS AUF VERWANDTE ANMELDUNGEN

[0001] Diese Anmeldung basiert auf den vorläufigen Anmeldungen 60/409,716, eingereicht am 10. September 2002 (Anwaltsnummer 7167-102P1), 60/409,715, eingereicht am 10. September 2002 (Anwaltsnummer 7167-103P), 60/429,919, eingereicht am 27. November 2002 (Anwaltsnummer 7167-104P), 60/433,254, eingereicht am 13. Dezember 2002 (Anwaltsnummer 7167-105P) und 60/484,692, eingereicht am 3. Juli 2003 (Anwaltsnummer 7167-106P) und beansprucht deren Priorität, die hier in ihrer Gesamtheit durch Bezugnahme eingeschlossen sind.

HINTERGRUND

[0002] Die Computerisierung und insbesondere die Internettechnologie haben einen immer größeren Zugriff auf Daten vorgesehen, die Finanzdaten, medizinische Daten, persönliche Daten, umfassen, und mit Mitteln vorgesehen, um finanzielle oder andere Transaktionen, in denen vertrauliche Daten aktualisiert oder ausgetauscht werden, zu beschleunigen.

Stand der Technik

[0003] Gewöhnlich werden Passwörter verwendet, um die Vertraulichkeit derartiger Daten aufrechtzuerhalten, wobei Passwörter jedoch häufig auf einem Geburtsdatum oder einer Telefonnummer basieren, die leicht zu erraten und daher überhaupt nicht sicher ist. Ferner kann sogar ein kompliziertes zufällig erzeugtes Passwort oft leicht gestohlen werden.

[0004] Auf Passwort basierende Datenzugriffssysteme sind somit verletzbar gegenüber kriminellem Angriff mit der resultierenden Gefahr und dem resultierenden Schaden für die Industrie wie auch die Wirtschaft und sogar das Leben der Leute. Demgemäß besteht ein Bedarf nach einem verbesserten Verfahren zum Sichern von Daten und Schützen dieser Daten vor unautorisiertem Zugriff.

[0005] Biometrische Daten können präzise Details umfassen, die schwierig zu nehmen jedoch leicht zu analysieren sind (wie beispielsweise eine Abfolge von Einzelheiten von Fingerabdrücken) oder können Gesamtmuster umfassen, die leicht zu nehmen jedoch schwierig zu analysieren sind (wie beispielsweise die räumlichen Eigenschaften benachbarter Fingerabdruckswindungen).

[0006] Es existieren Verschlüsselungsalgorithmen, die einen digitalen Schlüssel erfordern, der nur für autorisierte Benutzer verfügbar ist. Ohne den richtigen Schlüssel können die verschlüsselten Daten nur unter erheblichem Zeitaufwand und erheblichen Verarbeitungsressourcen in ein geeignetes Format entschlüsselt werden, und sogar dann nur, wenn bestimmte Eigenschaften der entschlüsselten Daten bekannt sind (oder zumindest vorhersagbar sind).

[0007] Die japanische veröffentlichte Patentanmeldung JP 60-029868, datiert auf den 15. Februar 1985 im Namen von Tamio SAITO lehrt ein individuelles Identifikationssystem, das eine Identitätskarte mit einem integrierten Speicher zur Registrierung verschlüsselter biometrischer Daten verwendet, die von dem Kartenhalter erhalten wurden. Die biometrischen Daten können einen Stimmenabdruck, Fingerabdruck, ein physikalisches Aussehen und/oder ein biologisches Assay sein. In Gebrauch werden die Daten auf der Karte gelesen und entschlüsselt zum Vergleich mit entsprechenden Daten, die von der die Karte vorweisenden Person genommen wurden. Ein derartiges System erlaubt, dass eine registrierte Person mit einem hohen Genauigkeitsgrad positiv identifiziert werden kann. Jedoch ist es, da die biometrischen Daten durch eine externe Ausrüstung erhalten und verarbeitet werden, schwierig, die auf der Karte gespeicherte Information gegen mögliche Änderung und/oder Identitätsdiebstahl zu schützen.

[0008] Es ist eine verbesserte Identifikationskarte vorgeschlagen worden, die einen datenbetriebenen Multiprozessorchip auf der Karte umfasst, um eine Hardware-Firewall vorzusehen, die die auf der Karte gespeicherten biometrischen Daten sowohl verschlüsselt als auch isoliert, wodurch ein wesentlich größerer Schutz gegen unautorisierte Änderung gespeicherten Daten vorgesehen wird. Jedoch wurde der eigentliche Übereinstimmungsprozess in demselben externen Leserterminal ausgeführt, das die originalen biometrischen Daten genommen hat, und war somit immer noch potentiell angreifbar gegenüber betrügerischer Manipulation von außen.

ZUSAMMENFASSUNG

[0009] Eine erste Ausführungsform einer Hochsicherheitsidentifikationskarte umfasst nicht nur einen On-Board-Speicher für die gespeicherten biometrischen Daten, sondern auch einen On-Board-Sensor zum Nehmen der originalen biometrischen Daten. Ein Fernauthentifizierungssystem weist eine sichere Datenbank auf, die die biometrischen Daten umfasst. Ein On-Board-Prozessor auf der Karte führt einen vorbereitenden Übereinstimmungsvorgang durch, um zu verifizieren, dass die genommenen biometrischen Daten mit den lokal gespeicherten biometrischen Daten übereinstimmen. Nur wenn eine positive lokale Übereinstimmung besteht, werden genommene Daten oder sensitive gespeicherte Daten an das Fernauthentifizierungssystem zur zusätzlichen Verifikation und Weiterverarbeitung übertragen. Als ein weiterer Schutz gegen böswilligen Angriff sind die

lokal gespeicherten Daten bevorzugt von den entfernt gespeicherten Daten verschieden, und die lokale Übereinstimmung und die Fernübereinstimmung werden bevorzugt unter Verwendung verschiedener Übereinstimmungsalgorithmen durchgeführt. Somit besteht sogar, wenn die Karte, die lokal gespeicherten Daten und/oder der lokale Terminal, mit dem die Karte verbunden ist, jemals gefährdet sind, eine hohe Wahrscheinlichkeit, dass das Fernautorisierungssystem immer noch in der Lage ist, das versuchte Eindringen zu detektieren.

[0010] Eine zweite Ausführungsform umfasst auch einen On-Board-Speicher für die gespeicherten biometrischen Daten, einen On-Board-Sensor zum Nehmen der originalen biometrischen Daten und einen On-Board-Prozessor, wobei jedoch bei dieser Ausführungsform der gesamte Übereinstimmungsprozess durch den On-Board-Prozessor durchgeführt wird, und sowohl die original genommenen biometrischen Daten als auch andere "private" Information, die in dem On-Board-Speicher gespeichert ist, für irgendwelche externen Prozesse nicht verfügbar gemacht werden. Stattdessen wird nur eine Verifikationsnachricht in Ansprechen auf eine erfolgreiche Übereinstimmung zwischen den neu genommenen biometrischen Daten und den vorher genommenen biometrischen Daten erzeugt. Die Verifikationsnachricht bewirkt, dass die Karte in einer Weise, die ähnlich einer herkömmlichen ISO-Chipkarte ist, bei dem erfolgreichen bzw. nicht erfolgreichen Eingeben einer herkömmlichen persönlichen Identifikationsnummer (PIN) funktioniert, jedoch mit der zusätzlichen Sicherheit, die durch einen sichereren Verifikationsprozess geboten wird. Bei jeder dieser Ausführungsformen werden die gespeicherten biometrischen Daten und jeglicher zugeordneter lokal gespeicherter Verschlüsselungsalgorithmus oder Verschlüsselungsschlüssel bevorzugt auf die Karte zu dem Zeitpunkt des ursprünglichen Ausgebens an den Kartenhalter in einer Weise geladen, die jeden nachfolgenden externen Zugriff abschreckt, wodurch die Integrität gespeicherter biometrischer Daten und des gesamten Verifikationsprozesses weiter gesteigert wird.

[0011] Bei einer Ausführungsform funktioniert die ISO-Chipkarte als eine Firewall zum Schützen des Sicherheitsprozessors, der zum Speichern und Verarbeiten der geschützten biometrischen Daten vor einem böswilligen externen Angriff über die ISO-Chipkarten-Schnittstelle verwendet wird. Bei einer anderen Ausführungsform ist der Sicherheitsprozessor zwischen die ISO-Chipkarten-Schnittstelle und einen nicht modifizierten ISO-Chipkarten-Prozessor eingesetzt und blockiert jegliche externe Kommunikationen solange, bis der Fingerabdruck des Benutzers mit einem vorher registrierten Fingerabdruck in Übereinstimmung gebracht worden ist.

[0012] Bei einer bevorzugten Ausführungsform einer Hochsicherheitsidentifikationskarte mit einer On-Board-Fingerabdruckübereinstimmfähigkeit wird eine Echtzeitrückkopplung vorgesehen, während der Benutzer seinen Finger über den Fingerabdrucksensor führt, wodurch eine optimale Anordnung des Fingers über dem Sensor erleichtert wird. Diese Rückkopplung reduziert nicht nur eine Berechnungskomplexität, sondern sieht auch ein zusätzliches Mittel zum Unterscheiden zwischen einem unerfahrenen Benutzer und einem betrügerischen Benutzer vor, wodurch die Wahrscheinlichkeit falscher Negative und/oder falscher Positive weiter verringert wird. Bei einer anderen bevorzugten Ausführungsform ist der Fingerabdrucksensor in einem Träger gehalten, der eine zusätzliche Steifigkeit vorsieht.

[0013] Bei einer beispielhaften Anwendung werden die genommenen biometrischen Daten und/oder eine Angabe der Identität des Kartenhalters verschlüsselt und in ein Transaktionsnetzwerk eingegeben, das eine Finanzinstitution und einen separaten Authentifizierungsserver umfasst, vor Erteilung eines Onlinezugriffs auf vertrauliche Daten oder einen automatisierten Prozess zum Beenden einer sicheren Transaktion. Bei einer anderen beispielhaften Anwendung wird die Ausgabe von der Karte dazu verwendet, einen physikalischen Zugang in einen sicheren Bereich zu erhalten. Bei jeder Anwendung kann eine Aufzeichnung erfolgreicher und nicht erfolgreicher Zugriffsversuche entweder auf der Karte oder einem externen Sicherheitsserver oder beiden gespeichert werden.

Ausführungsbeispiel

ZEICHNUNGEN

[0014] Fig. 1 zeigt eine Ausführungsform einer Chipkarte mit einer biometrischen On-Board-Verifikation der Identität der die Karte vorweisenden Person.

[0015] Fig. 2 ist ein Flussdiagramm, das einen beispielhaften Prozess zum Unterstützen des Benutzers bei der optimalen Anordnung eines Fingers auf dem Fingerabdrucksensor zeigt.

[0016] Fig. 3 ist ein funktionelles Blockschaubild eines biometrischen Verifikationssystems, das sowohl eine lokale als auch entfernte Verifikation der Identität einer Person, die eine sichere Identifikationskarte vorweist, durchführen kann.

[0017] Fig. 4 ist ein funktionelles Blockschaubild einer beispielhaften Karte für biometrische Verifikation, die verschiedene physikalische Datenpfade zur Verwendung während des anfänglichen Ladens der biometrischen Daten des Kartenhalters und während der Verifikation der Identität des Kartenhalters an eine Fernanwendung aufweist.

[0018] Fig. 5 zeigt eine zu der beispielhaften Karte für biometrische Verifikation von Fig. 4 alternative Ausführungsform, die zur Verwendung mit einer nicht modifizierten ISO-Chipkarten-CPU bestimmt ist.

[0019] Fig. 6 ist ein Flussdiagramm, das die Kommunikation zwischen einer beispielhaften Anwendung und einer beispielhaften Verifikationskarte zeigt, bei der nur eine lokale Verifikation der Identität des Kartenhalters ausgeführt wird.

[0020] Fig. 7 ist ähnlich des Flussschaubilds von Fig. 6, jedoch zur Verwendung mit der beispielhaften Karte mit biometrischer Verifikation von Fig. 5 abgewandelt.

[0021] Fig. 8 zeigt eine zweite Ausführungsform einer Chipkarte mit einer biometrischen On-Board-Verifikation, die mit einem lokalen Terminal entweder drahtlos oder über einen elektrischen Verbinder verbunden sein kann.

[0022] Fig. 9 ist ein Schnitt durch die Karte von Fig. 8.

[0023] Fig. 10 ist ein Schaltbild eines beispielhaften Fingerabdrucksensors.

[0024] Fig. 11 zeigt eine Ausführungsform eines Trägerzusammenbaus für den Sensor von Fig. 10.

DETAILLIERTE BESCHREIBUNG

Chipkarte

[0025] Der Begriff "Chipkarte" oder "intelligente Karte" ist hier in einem allgemeinen Sinne verwendet, um jegliches physische Objekt zu bezeichnen, das klein genug ist, damit es in der Hand gehalten, um den Hals getragen oder anderweitig an der Person getragen werden kann und das einen Mikroprozessor umfasst, der in der Lage ist, digital codierte Information zu speichern, zu verarbeiten und zu kommunizieren, die den individuellen Kartenhalter betrifft oder anderweitig mit diesem in Verbindung steht. Ein gut bekanntes Beispiel einer derartigen Chipkarte ist die ISO (International Standards Organization) Chipkarte, die dieselbe physikalische Größe und Form einer herkömmlichen Kreditkarte besitzt, jedoch einen Flashspeicher zur Speichern von nutzerspezifischen Daten und einem Mikroprozessor umfasst, der mit einem leistungsfähigen Verschlüsselungsalgorithmus programmiert sein kann, der angibt, ob eine PIN (persönliche Identifikationsnummer), die von einem Benutzerterminal erhalten wurde, mit einer verschlüsselten PIN, die auf der Karte gespeichert ist, übereinstimmt, wodurch ein höherer Grad an Vertrauen vorgesehen wird, dass die die Karte vorweisende Person der echte Kartenhalter ist, als es bei einem Verifikationssystem möglich wäre, das sich nur auf einen visuellen Vergleich von Signaturen und/oder physischer Ähnlichkeit verlässt.

[0026] Fig. 1 zeigt eine Ausführungsform einer Chipkarte mit einer biometrischen On-Board-Verifikation. Die Karte **100** ist allgemein aus einem Kunststoffmaterial gefertigt und besitzt das Gesamtaussehen einer herkömmlichen Kreditkarte mit ungefähren Abmessungen, wie in ISO 7816 festgelegt ist, von etwa 53,98×85,6 mm und einer Dicke von 0,76 mm oder darüber.

[0027] Ähnlich einer herkömmlichen Kreditkarte umfasst die Karte **100** ein freies oberes Gebiet **102**, das sich entlang der gesamten Querbreite der Karte erstreckt, um einen Magnetstreifen (wie durch ISO 7811-2 & 7811-6) festgelegt ist, auf der Rückfläche der Karte zu tragen, auf dem herkömmlich codierte alphanumerische Information über den Kartenhalter wie auch ein zugeordnetes Konto gespeichert sein kann, wodurch die Karte **100** in einem herkömmlichen Magnetstreifenleser verwendet werden kann. Jedoch ist, da in dem Magnetstreifen eingebettete Daten leicht geändert werden können, ein derartiger Magnetstreifen nur zur Verwendung bei bestimmten Anwendungen bestimmt, bei denen der Bedarf nach Rückwärtskompatibilität mit älteren magnetstreifenbasierten Terminals die potentielle Abnahme der Sicherheit, die ein Magnetstreifen für das System mit sich bringt, überwiegt.

[0028] Das obere Gebiet **102** kann auch dazu verwendet werden, verschiedene Maßnahmen zum Verhindern von Betrug zu tragen, wie beispielsweise eine manipulationsbeständige Farbfotografie des Kartenhalters und/oder ein holografisches Logo des Kartenherausgebers. Das untere Gebiet **104** der Karte **100** kann in einer herkömmlichen Art und Weise für geprägte Information verwendet werden (wie durch ISO 7811-1) festgelegt ist, wie beispielsweise den Namen des Kartenhalters, eine numerische Konto-(oder Karten-)Identifizierung und ein Ablaufdatum, um die Verwendung der Karte **100** in einem herkömmlichen Kartenpräge- und Druckwerkzeug zuzulassen.

[0029] Das obere Gebiet **102** und das untere Gebiet **104** sind durch ein mittleres Gebiet **106** getrennt, in dem ein Satz von 8 sichtbaren ISO-Chipkarten-Kontaktstellen **108** eingebettet ist, die eine geeignete elektrische Verbindung zwischen der Karte und entsprechenden Kontakten an einem Kartenleser vorsehen. Durch dieses Mittel können nicht nur Daten sondern auch Strom, Zeit- bzw. Takt- wie auch Steuersignale zwischen dem Leser und der Karte ausgetauscht werden, wie in ISO 7816-3 festgelegt ist.

[0030] Auf der rechten Seite des Gebiets **106** ist ein Sensorpolster **110** sichtbar, das dazu verwendet wird, Fingerabdruckdaten von dem Finger eines Kar-

tenhalters zu nehmen. Die Karte ist bevorzugt mit einem ID-Code versehen, der einmalig für den Sensor **110** oder eine andere elektronische Komponente, die in der Karte eingebettet ist, ist, beispielsweise ein Code in dem Format einer herkömmlichen IP- und/oder MAC-Adresse.

[0031] Ebenfalls in Fig. 1 sind verschiedene zusätzliche elektronische Komponenten gezeigt, die mit der Kontaktstelle **108** und dem Sensor **110** zusammenwirken, um eine größere Funktionalität und insbesondere eine bessere Sicherheit vorzusehen, als es ansonsten möglich wäre.

[0032] Bei einer Ausführungsform ist ein ISO-Chipkartenkompatibler Prozessor **112** direkt mit den ISO-Kontaktstellen **108** verbunden, um eine elektrische Verbindung mit einem externen ISO-kompatiblen Kartenleser (nicht gezeigt) vorzusehen, wodurch nicht nur Strom an die On-Board-Elektronik geliefert wird, sondern auch ein Mittel zum Kommunizieren von Daten zwischen der Karte und externer Kommunikationssoftware, Sicherheitssoftware, Transaktionssoftware und/oder anderer Anwendungssoftware bereitgestellt wird, die auf dem Kartenleser oder zugeordneten Berechnungsvorrichtungen, die sich in einem Netzwerk mit dem Kartenleser beifinden, läuft.

[0033] Obwohl bei der gezeigten Ausführungsform der Datenpfad zwischen der Karte **100** und dem externen Kartenleser in der Form einer verdrahteten Verbindung unter Verwendung einer ISO-spezifizierten Chipkarten-Kontaktanordnung vorgesehen ist, sei zu verstehen, dass bei anderen Ausführungsformen andere Übertragungstechnologien ebenfalls verwendet werden können, wie beispielsweise USB- oder RS 232C- oder SPI-(Seriell)-Verbindungen, möglicherweise über drahtlose HF (Hochfrequenz), Mikrowellen- und/oder IR-(Infrarot)-Kommunikationsverbindungen.

[0034] Auch könnten, obwohl die oben beschriebene Ausführungsform Strom von dem Kartenleser aufnimmt, andere Ausführungsformen eine On-Board-Energiequelle besitzen, wie beispielsweise eine Solarzelle oder eine Batterie. Eine derartige On-Board-Energiequelle könnte vorteilhaft sein, beispielsweise wenn die mechanische Schnittstelle zwischen der Karte **100** und einem bestimmten Typ von Kartenleser derart ist, dass der Fingerabdrucksensor **110** für den Benutzer nicht zugänglich ist, wenn die Kontakte **108** mit den entsprechenden Verbindungen in dem Kartenleser verbunden sind, und somit die Fingerabdruckdaten des Benutzers genommen werden müssen, wenn die Karte **100** nicht direkt mit dem Kartenleser verdrahtet ist.

Sicherheitsprozessor

[0035] Wie gezeigt ist, ist der Sicherheitsprozessor **114** zwischen den ISO-Prozessor **112** und den Sensor **110** geschaltet, um eine sichere Verarbeitung und Speicherung der genommenen Daten wie auch eine sichere "Firewall" vorzusehen, um die Daten und Programme, die in ihrem dedizierten Speicher gespeichert sind, vor einem unrichtigen Zugriffsversuch über den ISO-Prozessor **112** zu schützen, wie nachfolgend beschrieben ist. Eine derartige Firewall kann so ausgebildet sein, dass sie nur verschlüsselte Daten unter Verwendung eines Verschlüsselungsschlüssels durchlässt, der auf einer einmalig zugewiesenen Netzwerkadresse basiert oder der ansonsten für die bestimmte Karte einmalig ist, wie beispielsweise Daten, die von einem vorher gespeicherten Fingerabdruckmuster oder einer einmalig zugewiesenen Vorrichtungsnummer, wie z.B. einer CPU-Nummer oder einer Fingerabdruckssensornummer, extrahiert sind. Bei einer anderen Ausführungsform lässt die Firewall nur Daten durch, die einzigartige Identifikationsdaten von einer vorhergehenden Übertragung oder Daten enthält. Bei noch anderen Ausführungsformen weist die Firewall verschiedene Schlüssel für verschiedene Anwendungen auf und verwendet diese Schlüssel, um die Daten an einen jeweiligen anderen Prozessor oder eine andere Speicherpartition zu führen.

[0036] Bei einer anderen Ausführungsform (nicht gezeigt) ist der Sicherheitsprozessor **114** direkt mit den ISO-Kontakten **108** verbunden und wirkt als ein sicherer Pförtner zwischen dem ISO-Prozessor **112** und den ISO-Kontakten **108**. Eine derartige alternative Anordnung besitzt den Vorteil, dass eine zusätzliche Sicherheit vorgesehen wird, die durch den Sicherheitsprozessor **114** und den Sensor **110** geboten wird, ohne mögliche Beeinträchtigung von Sicherheitsmerkmalen, die bereits in dem ISO-Prozessor **112** integriert sein können.

[0037] Der Sicherheitsprozessor **114** umfasst bevorzugt einen nichtflüchtigen Halbleiter- oder Nichthalbleiterspeicher, wie beispielsweise einen FRAM, OTP, E^2PROM, MRAM, MROM zum Speichern eines vorher eingetragenen Fingerabdruckmusters und/oder anderer persönlicher biometrischer Informationen. Bei anderen Ausführungsformen könnten einige oder alle Funktionen des Sicherheitsprozessors **114** in dem ISO-Prozessor **112** implementiert sein und/oder einige oder alle Funktionen des ISO-Prozessors **112** könnten in dem Sicherheitsprozessor **114** implementiert sein. Eine derartige kombinierte Implementierung könnte immer noch eine Softwarefirewall zwischen den verschiedenen Funktionen aufrechterhalten, was insbesondere vorteilhaft wäre, wenn die Vorrichtung mit einem Prozess implementiert wäre, der keine nachfolgende Abänderung an den gespeicherten Softwareprogrammen zulässt. Alternativ dazu könnten beide Prozessoren **112**, **114** separate Prozessoren in einer einzelnen Multiprozessorvorrichtung sein, die derart ausgebildet ist, um

jeden Prozess vor einer Überlagerung von einem anderen Prozess, der in einem anderen Prozessor läuft, zu schützen. Ein Beispiel einer derartigen Multiprozessorvorrichtung ist der DDMP (Data Driven Multiple Processor) von Sharp in Japan.

[0038] Obwohl diese verschiedenen Sensoren, Kontakte und anderen elektronischen Komponenten wie auch die gedruckten Schaltungen oder andere elektrische Verdrahtung, mit denen sie verbunden sind, bevorzugt alle vollständig innerhalb des Körpers der Karte **100** integriert sind, so dass sie vor Abrieb und externen Schmutzstoffen geschützt sind, schützt die bevorzugte Anordnung in dem mittleren Gebiet **106** zwischen dem oberen Gebiet **102** und dem unteren Gebiet **104** diese ferner vor einem möglichen Schaden von den herkömmlichen Magnetstreifenlesern, Stanzeinrichtungen wie auch Druck- bzw. Prägeausstattung, die mechanisch mit diesen anderen Gebieten in Kontakt treten.

LED-Rückkopplung

[0039] LEDs **116a**, **116b** werden von dem Sicherheitsprozessor **114** gesteuert und sehen eine sichtbare Rückkopplung für den Benutzer vor. Bei der gezeigten Ausführungsform sind diese in dem unteren Gebiet **104** bevorzugt an einem Ort an dem Seitenrand der Karte entfernt von den Kontaktstellen **108** angeordnet. In jedem Fall sind die LEDs **116a**, **116b** bevorzugt dort angeordnet, wo sie während eines Stanzprozesses nicht beschädigt werden können und wo sie sichtbar sind, wenn die Karte in einen herkömmlichen ISO-Chipkarten-Leser eingesetzt ist und/oder während der Finger des Benutzers über dem Fingerabdrucksensor **110** angeordnet ist. Beispielsweise:

In der Verifikationsbetriebsart:

- ROT blinkt: Warten auf Finger
- Stopp des Blinkens: Finger liegt auf Sensor
- ROT blinkt einmal: Übereinstimmung nicht feststellbar, OK zur Bewegung des Fingers
- GRÜN langes Blinkzeichen einmal: Übereinstimmung, OK zum Bewegen des Fingers

In der Eintragbetriebsart

- GRÜN blinkt: Warten auf Finger
- Stopp des Blinkens: Finger liegt auf Sensor
- ROT blinkt einmal: Eintragen nicht durchführbar, OK zum Bewegen des Fingers
- GRÜN blinkt einmal: Eingetragen, OK zum Bewegen des Fingers

In der Löschbetriebsart

- GRÜN und ROT blinkt: Bereit zum Löschen
- GRÜN blinkt einmal: Gelöscht

[0040] Dem Benutzer werden bevorzugt mehrere Möglichkeiten zum Positionieren seines Fingers für eine erfolgreiche Übereinstimmung oder Eintragung gegeben, bevor ein negativer Bericht übertragen wird. Bei einer Ausführungsform wird ein negativer Bericht an den Authentifizierungsserver nur dann übertragen, wenn der Benutzer seinen Finger bewegt hat, bevor die grüne OK-Anzeige erhalten wurde, oder wenn eine vorbestimmte Zeitbeschränkung überschritten worden ist. Ein derartiger Prozess führt nicht nur den Benutzer, um eine optimale Anordnung seines Fingers über dem Sensor zu machen, was nicht nur die Berechnungskomplexität verringert, sondern lässt auch die Verwendung mehrerer Unterscheidungsschwellen zu. Diese sichtbare Rückkopplung sieht auch eine psychologische Basis zur Unterscheidung zwischen einem nicht erfahrenen Benutzer (der typischerweise so lange versucht, bis er die richtige Positionierung erreicht) und einem betrügerischen Benutzer vor (der typischerweise keine Aufmerksamkeit auf sich ziehen möchte und aufhört, bevor seine böswilligen Absichten entdeckt werden). Das Nettoergebnis ist eine erhebliche Verringerung der Wahrscheinlichkeit falscher Negative und/oder falscher Positive.

[0041] Fig. 2 zeigt einen beispielhaften Prozess zum Unterstützen des Benutzers beim Anordnen seines Fingers auf dem Sensor **110**. Bei Block **150** blinkt die ROT-LED **116b**. Sobald ein Finger erfasst worden ist (Block **152**) stoppt die LED das Blinken und ein Test (Block **154**) wird zur Bildqualität ausgeführt (definierte längliche Gebiete entsprechend den Bergen und Tälern der Haut des Fingers). Wenn die Qualität nicht angemessen ist (NEIN-Zweig **156**), weist ein einzelnes Blinkzeichen der ROT-LED **116b** den Benutzer an, seinen Finger in eine andere Position zu bewegen (Block **158**); ansonsten (JA-Zweig **160**) wird ein zweiter Test (Block **162**) ausgeführt, um zu bestimmen, ob derselbe Finger in derselben Position angeordnet wurde, wie dazu verwendet wurde, den Benutzer einzutragen, so dass ein relativ einfacher Übereinstimmungsalgorithmus verifizieren kann, dass die aktuellen Daten den gespeicherten Daten innerhalb einer vorbestimmte Schwelle entsprechen, wodurch verifiziert wird, dass der aktuelle Finger derselbe Finger ist, wie der Finger, der ursprünglich eingetragen wurde (JA-Zweig **164**), und die GRÜN-LED **116a** wird (Block **166**) für eine ausreichende Zeit (Block **168**) aktiviert, um zu verifizieren, dass eine erfolgreiche Übereinstimmung durchgeführt wurde und der Benutzer nun seinen Finger wegnehmen kann. Wenn alternativ dazu die Übereinstimmungsschwelle nicht erfüllt ist (NEIN-Zweig **170**), weist ein einzelnes Blinkzeichen der ROT-LED **116b** (Block **158** den Benutzer an, seinen Finger in eine andere Position zu bewegen, und der Prozess wird wiederholt.

BEISPIELHAFTE NETZWERKARCHITEKTUREN

[0042] Fig. 3 zeigt eine mögliche Ausführungsform eines biometrischen Verifikationssystems, das sowohl eine lokale als auch entfernte Verifikation der Identität einer Person durchführen kann, die eine sichere Identifikationskarte vorweist. Sie umfasst drei Hauptkomponenten: einen Client-Terminal **200**, einen Anwendungsserver **202** und einen Authentifizierungsserver **204**. Der Client-Terminal **200** umfasst eine Funktionalität zum aktuellen Nehmen und lokalen Verarbeiten eines Fingerabdrucks eines Benutzers, zum Verschlüsseln der lokal verarbeiteten Daten und zur sicheren Kommunikation mit dem Anwendungsserver und dem Authentifizierungsserver bevorzugt über das Internet unter Verwendung des IP/TCP-Adressschemas und -übertragungsprotokolls, wobei ein Schutz vor böswilligem Zugriff durch herkömmliche IP-Firewalls **206** vorgesehen wird. Bei anderen Ausführungsformen können die Firewalls **206** mit Filtern und Verschlüsselungscodierern bzw. -decodierern versehen sein, die übertragene Daten codieren, nachdem diese mit den autorisierten Daten verifiziert worden sind, und die empfangene Daten decodieren, bevor entschieden wird, ob es sich tatsächlich um autorisierte Daten handelt, beispielsweise unter Verwendung eines Verschlüsselungsalgorithmus, wie z.B. DES **128**. Durch dieses Mittel kann die Firewall **206** Daten als autorisiert oder potentiell böswillig auf Grundlage nicht nur des Nachrichtenkopfes sondern auch auf Grundlage des Nachrichteninhalts klassifizieren.

[0043] Der Client-Terminal **200** kann als eine dedizierte Web-Anwendung implementiert sein oder kann in Software implementiert sein, die auf einem programmierbaren Desktop, Notebook oder anderer Workstation oder Personalcomputer installiert ist, der durch ein Allzweckbetriebssystem gesteuert wird, wie beispielsweise Windows XXX, OS X, Solarris XX, Linux oder Free BSD. Der Client-Terminal **200** umfasst bevorzugt aktuelle "negative" Datenbanken (beispielsweise Identitäten von verlorenen oder gestohlenen Karten oder Beschränkungen bezüglich einer bestimmten Karte oder einer Gruppe von Karten), die ein zusätzliches Maß an Sicherheit bieten.

[0044] Der Anwendungsserver **202** umfasst eine Funktionalität zum Durchführen einer Transaktion oder einem anderweitigen Reagieren auf Anweisungen von dem entfernten Benutzer an dem Client-Terminal **200**, nachdem die Identität des Benutzers durch den Authentisierungsserver **204** verifiziert worden ist. Der Authentisierungsserver **204** umfasst eine Funktionalität zur sicheren Verbindung mit dem sowohl dem Client-Terminal **200** als auch dem Anwendungsserver **202** zum Speichern authentischer Fingerabdruckdaten und anderer Information betreffend vorher registrierten Benutzern zum Vergleich der gespeicherten Daten mit den verschlüsselten aktuellen Daten, die von dem Client-Server **200** empfangen wurden, und zum Beraten des Anwendungsservers **202**, ob die spezifizierten aktuellen Fingerabdruckdaten mit spezifizierten gespeicherten Fingerabdruckdaten übereinstimmen oder nicht.

[0045] Insbesondere umfasst der Client-Terminal **200** ferner zwei Hauptkomponenten: eine fixierte Kartenleserkomponente **208** mit einem Internetbrowseranschluss **210** und einer Kartenleserschnittstelle **108a** (die ein einfaches USB-Kabel sein kann, das in einem Satz elektrischer Kontakte endet, um eine jeweilige elektrische Verbindung mit ISO-Chipkarten-Kontaktstellen **108** zu bilden) und eine tragbare Chipkartenkomponente **100'**. Bei einer Ausführungsform kann die tragbare Komponente **100'** die vorher beschriebene Chipkarte **100** mit dem Fingerabdrucksensor **110**, dem Sicherheitsprozessor **114** und dem ISO-Chipkarten-Prozessor **112** sein.

[0046] Der Anwendungsserver **202** umfasst ferner eine Internetserverschnittstelle mit der Firewall **206** und dem Internetbrowser **214**, wie auch ein Transaktionsanwendungsmodul **216** und ein Validierungsmodul **218**. In dem Fall, dass der Anwendungsserver und das Anwendungsmodul **216** Legacy-Devices sind, die nicht dazu ausgebildet wurden, extern mittels des IP/TCP-Protokolls zu kommunizieren, kann die Firewall **206** durch einen geeigneten Protokollumwandler ersetzt werden, der das Validierungsmodul **218** integriert und eine fixierte IP-Adresse besitzt. Der Anwendungsdienstserver kann beispielsweise durch eine dritte Partei betrieben werden, die willens ist, einen Dienst durch das Internet für einen autorisierten Benutzer bereitzustellen.

[0047] Der Authentifizierungsserver **204** umfasst ferner eine Internetdienstschnittstelle **220**, ein Verarbeitungsmodul **222** mit einem Fingerabdruckübereinstimmalgorithmus **224** und eine Datenbank **226** zum Speichern von Fingerabdrücken und anderer authentischer Information, die von Personen zu dem Zeitpunkt gesammelt wurde, zu dem derartige Personen in dem System registriert wurden und ihre Identität zur Zufriedenstellung des Systembedieners garantiert wurde. Als eine weitere Sicherheitsverbesserung werden die gespeicherten Daten für eine bestimmte Person bevorzugt nicht auf dem Benutzerserver als eine einzelne Abfolge von Information gespeichert, sondern vielmehr wird jedes Element separat gespeichert und die erforderlichen Indizes oder Beziehungen, die diese Elemente verbinden, sind nur mittels eines entsprechenden Schlüssels zugänglich, der als Teil dieser privaten Daten der Person in dem Authentifizierungsserver gehalten wird.

Ort

[0048] Bei bestimmten Ausführungsformen können der fixierte Leser **208** und/oder die tragbare Karte

100" auch mit einem integralen Seitennavigationssystem- ("GPS")-Empfänger ausgestattet sein, der nützliche Information über den gegenwärtigen Ort des Lesers und der Karte zu oder etwa der Zeit vorsehen kann, zu der eine bestimmte Transaktion stattfindet. Insbesondere können die Ortsdaten von dem GPS-Empfänger **212** dazu verwendet werden, den Leser und/oder die Karte in dem Falle (entweder permanent oder temporär) außer Betrieb zu setzen, wenn einer oder beide derselben an einen Ort entfernt werden, an dem ihre Verwendung nicht autorisiert ist. Eine Position kann auch automatisch durch andere Vorrichtungen als GPS bestimmt werden, beispielsweise unter Verwendung von PHS- (japanisches zelluläres Telefon) Anruferorttechnologie oder Ortsensoren, die auf örtliche Änderungen in den elektromagnetischen Feldern der Erde ansprechen. In dem bestimmten Fall einer mit GPS ausgestatten Karte sind die verschiedenen GPS-Komponenten, die Antennen; Signalverstärkung, AD-Wandler und Abtast- und Halteschaltungen; und einen Digitalprozessor zur Berechnung der Position umfassen, bevorzugt alle Teil einer einzelnen integrierten Schaltung oder diskreter Vorrichtungen, die an einer einzelnen Leiterplatte befestigt sind, die in den Körper der Karte integriert, in diesen eingebettet oder in diesen laminiert ist.

Kartenarchitektur für ISO-Karte mit On-Board-Übereinstimmung

ISP-Prozessorschnittstellen

[0049] Fig. 4 ist ein funktionelles Blockschaubild einer beispielhaften ISO-Chipkarten-kompatiblen Karte **100** oder **100'** mit biometrischer Verifikation mit verschiedenen physikalischen Datenpfaden zur Verwendung während eines anfänglichen Ladens der biometrischen Daten des Kartenhalters und während der Verifikation der Identität des Kartenhalters zu einer entfernten Anwendung.

[0050] Insbesondere ist zusätzlich zu dem vorher beschriebenen ISO-Prozessor **112**, Sicherheitsprozessor **114**, Fingerabdrucksensor **110**, den LEDs **116a**, **116b** und dem optionalen GPS-Empfänger **212**, wobei nur der ISO-Prozessor **112** direkt mit dem Kartenleser **208** über die ISO-Chipkarten-Kontaktstellen **108** verbunden ist, ein separates Lademodul **300** und eine zugeordnete temporäre Verbindung **302** gezeigt, die für eine direkte Verbindung mit dem Sicherheitsprozessor **114** während der anfänglichen Benutzerregistrierung sorgt. Es sei angemerkt, dass der ISO-Prozessor **112** mit dem Sicherheitsprozessor **114** über I/O-Ports **304**, **306** in Verbindung steht, während die temporäre Ladeverbindung **302** mit einem separaten I/O-Port **308** verbunden ist. Der Sicherheitsprozessor ist bevorzugt derart programmiert, dass jegliche sensitiven sicherheitsrelevanten Daten oder Software nur von dem Port **308** und nicht von den Ports **304** und **306** zugänglich sind, wodurch die Wahrscheinlichkeit eines böswilligen Zugriffs auf diese sensitiven Daten vermieden wird, nachdem die Verbindung **302** außer Betrieb genommen wurde.

[0051] Der größte Teil der kommerziell verfügbaren ISO-Prozessoren besitzt zumindest zwei I/O-Ports und einige besitzen zumindest drei. Nur einer dieser Ports (I/O 1) ist für die herkömmliche ISO-Chipkarten-Seriellдatenverbindung **108** zu dem externen ISO-kompatiblen Kartenleser **208** vorgesehen. Der zusätzliche eine oder die zusätzlichen beiden I/O-Ports sehen bevorzugt eine dedizierte hartverdrahtete Verbindung zwischen dem ISO-Prozessor **112** und dem Sicherheitsprozessor **114** vor, die als eine Hardwarefirewall wirkt, um jegliche böswillige Versuche zum Umprogrammieren des Sicherheitsprozessors **114** oder zum Erzielen von Zugriff auf sensitive Information zu blockieren, die vorher von dem Sensor **110** genommen worden sein kann oder die ansonsten in dem Prozessor **114** gespeichert sein kann. In dem bestimmten Fall eines ISO-Prozessors mit mehr als zwei I/O-Leitungen ist es möglich, mehr als zwei Zustände von statischer Statusinformation an dem dedizierten Kommunikationspfad zwischen dem ISO-Prozessor und dem Sicherheitsprozessor anzubieten, z. B. 1) Bereit, 2) in Betrieb, 3) Ausfall und 4) Durchlass, sogar, wenn der Sicherheitsprozessor vollständig heruntergefahren ist. Selbstverständlich können sogar, wenn nur ein I/O-Port verfügbar ist, diese vier Zustände dynamisch als serielle Daten übertragen werden.

[0052] Unter den möglichen Anweisungen und Daten, die zwischen der ISO-CPU und der Sicherheits-CPU über die ISO-Schnittstellen I/O 2 und I/O 3 übertragen werden können, sind die folgenden:

- Anweisungen, um einen Benutzer einzutragen oder zu authentifizieren, an den die Sicherheits-CPU das Ergebnis des Eintragens oder das Ergebnis der Authentifizierung zur lokalen Speicherung und/oder Übertragung an eine entfernte Anwendung sendet.
- Fingerabdruckinformation kann als eine Vorlage (Referenz) von der Sicherheits-CPU an die ISO-CPU zur Speicherung in dem ISO-Smart-Cart-Speicher zur Übertragung an entfernte Anwendungen gesendet werden. Zur erhöhten Sicherheit sensitiver persönlicher Information können die Referenzdaten durch die Sicherheits-CPU verschlüsselt werden, bevor sie an die ISO-CPU gesendet werden.

[0053] Die Ladeverbindung **302** sieht eine direkte Verbindung mit der Sicherheits-CPU **114** vor, die jeglichen Firewallschutz umgeht, der von der ISO-Verbindung und den zugeordneten dedizierten I/O-Ports **304** und **306** angeboten wird, während möglicherweise eine Kommunikation zwischen der ISO-CPU **112** und dem ISO-Leser **208** aufrecht erhalten wird, so

dass Strom auch für die Sicherheits-CPU **114** verfügbar ist. Sie wird hauptsächlich während der anfänglichen Registrierung der Karte für einen bestimmten Benutzer verwendet und sollte gegen unauthorisierten Zugriff geschützt werden.

[0054] Fig. 5 zeigt eine für die beispielhafte Karte mit biometrischer Verifikation von Fig. 4 alternative Ausführungsform, die zur Verwendung mit einer nicht modifizierten ISO-Chipkarten-CPU bestimmt ist. Insbesondere muss die ISO-CPU **112'** nicht mehr irgendwelche Gatewayfunktionen zwischen dem Kartenleser **208** und der Sicherheits-CPU **114'** entweder während des normalen Gebrauchs oder während des Ladens ausführen und kann somit ein beliebiger nach ISO anerkannter Chip sein, der nicht modifiziert ist und nur in einer Weise verwendet wird, die absolut transparent für sowohl den Kartenleser **208** als auch die externe Anwendung ist. Bei einer derartigen alternativen Ausführungsform wirkt die Sicherheits-CPU **114'** als eine transparente Firewall zwischen der ISO-CPU **112'** und einer externen Anwendung, wenn der genommene Fingerabdruck mit dem gespeicherten Fingerabdruck übereinstimmt, und blockiert alle derartigen Kommunikationen, wenn der genommene Fingerabdruck nicht mit dem gespeicherten Fingerabdruck übereinstimmt.

Karteninitialisierung und Schutz von gespeicherten Daten

Guillotine

[0055] Bei einer Ausführungsform besitzt die ursprünglich hergestellte Karte eine vorragende Leiterplattenverlängerung, die eine direkte Verbindung mit der Sicherheits-CPU wie auch mit zumindest Abschnitten der ISO-Schnittstelle und/oder einem diskreten On-Board-Speicher vorsieht. Diese Direktverbindungsschnittstelle wird nur zum Testen der Karte und zum Eintragen von Fingerabdruck verwendet und umfasst das Signal, das den Eintragungsprozess erlaubt. Nachdem das Eintragen beendet worden ist, wird diese Leiterplattenverlängerung mechanisch abgetrennt, so dass keine weitere Eintragung mehr möglich ist und der Sicherheits-CPU-Speicher nur durch die ISO-CPU und die vorher erwähnte Firewall zwischen der ISO-CPU und der Sicherheits-CPU zugänglich ist.

Schmelzsicherung

[0056] Bei einer anderen Ausführungsform besitzt die Sicherheits-CPU einen Typ von Speicher, der, sobald das eingetragene Fingerabdruckmuster geschrieben ist, dann nicht mehr zugänglich ist. Ein Beispiel eines derartigen Speichers ist ein Einmal-PROM ("OTP"), der im Aufbau ähnlich dem EEPROM ist, jedoch für UV undurchlässig ist und somit nicht gelöscht werden kann. Ein anderes Beispiel ist ein Flash-ROM, der nur gelesen werden kann, nachdem das Eintragen beendet worden ist, beispielsweise durch Anlegen eines ausreichenden Stromes an einen Abschnitt des Aktivierungs- oder Adress- oder Datensignalpfads, um eine physikalische Unterbrechung ("Schmelzsicherung") in diesem Signalpfad zu bilden.

Beispielhafte Authentifizierungsprozesse

[0057] Bei einer Ausführungsform betrifft ein beispielhafter Authentifizierungsprozess das Nehmen physikalischer Fingerabdruckdaten beispielsweise unter Verwendung optischer oder druckbezogener oder leitender oder kapazitiver oder akustischer oder elastischer oder fotografischer Technologien an dem Client-Terminal, der von der zugreifenden Person zur Verbindung mit dem Anmeldungsdienstserver verwendet wird, die anschließend (bevorzugt in einer verschlüsselten Form) an einen separaten Fingerabdruckauthentifizierungsserver gesendet wird. Der Fingerabdruckauthentifizierungsserver vergleicht die genommenen Fingerabdruckdaten mit einer Fingerabdruckdatei, die die registrierten Fingerabdruckdaten von dem Benutzer umfasst, unter Verwendung einer Authentifizierungssoftware, und wenn die Daten übereinstimmen, sendet der Authentifizierungsserver eine Aktivierungsanweisung an den Anwendungsdienstserver.

[0058] Bei einer anderen Ausführungsform greift der Benutzer auf den gesicherten Web-Browser des Fingerabdruckauthentifizierungsservers zu, der Dateien von Fingerabdrücken enthält, in denen alle Fingerabdrücke zusammen mit individuellen Daten, wie beispielsweise Name, Adresse und Geburtsdatum vorregistriert sind. Der gesicherte Fingerabdruckauthentifizierungsserver, auf den der Benutzer durch ein sicheres Protokoll, wie beispielsweise dem HTTPS-Format zugreift, sendet dann eine Anweisung an den Client-Terminal, um den Fingerabdruck des Benutzers an dem Client-Terminal zu nehmen. In Ansprechen auf Anweisungen, die von dem Browser des Client-Terminals angezeigt werden, legt der Benutzer seinen gewählten Finger auf den Fingerabdrucksensor, und die Fingerabdrucknehmersoftware, die in dem Client-Terminal vorhanden ist, nimmt einen digitalen Fingerabdruck, beispielsweise ein auf Pixel basierendes Bild mit einer Auflösung mit einer Teilung von 25 Mikrometer zu 70 Mikrometer und einer Fläche von 12,5 mm im Quadrat bis zu 25 mm im Quadrat und ferner mit einer 8-Bit-Grauskala.

[0059] Der, sichere Fingerabdruckauthentifizierungsserver empfängt die Fingerabdruckdaten zusammen mit der User-ID wie auch der Internet-IP-Adresse und/oder dem individuellen Fingerabdrucksensorcode (MAC-Adresse) und/oder Cookie und/oder einem beliebigen einmaligen Code oder anderer Information, die die bestimmte Person oder den

bestimmten Terminal identifiziert (beispielsweise Details von einer vorhergehenden Konversation zwischen Client-Terminal und gesicherten Fingerabdruckauthentifizierungsserver), woraufhin dieser die empfangenen Fingerabdruckdaten mit einer Fingerabdruckdatei, die die vorregistrierten Fingerabdruckdaten zusammen mit der User-ID, individueller Information, wie beispielsweise Name, Adresse, Geburtsdatum, polizeilichem Führungszeugnis, Führerschein, Sozialsicherheitsnummer, etc., unter Verwendung einer Authentifizierungssoftware vergleicht, was ein Einzelheitenvergleich oder ein Vergleich mit Fast-Fourier-Transformation sein kann.

[0060] Zu Beginn des Authentifizierungsprozesses weist der Webserver **214** für die relevante Anwendung visuell oder hörbar den Benutzer an, seinen Finger auf den Fingerabdrucknehmersensor **110** zu legen und seinen Mausknopf oder eine Taste der Tastatur zu drücken und dadurch in Kontakt mit der Fingerabdrucknehmersoftware in dem Sicherheitsprozessor **114** zu kommen. Anschließend werden die Daten des genommenen Fingerabdrucks des Benutzers in verschlüsseltem Format (beispielsweise unter Verwendung des sicheren verschlüsselten RSA-Übertragungsprotokolls HTTPS) an den Webserver **220** des Fingerabdruckauthentifizierungsservers **204** über den ISO-Prozessor **112** und den Webbrowser **210** des Client-Terminals **200** gesendet. Wenn die genommenen Daten erfolgreich mit entsprechenden Daten in dessen Datenbank **226** in Übereinstimmung sind, validiert der Fingerabdruckauthentifizierungsserver **204** dann die Identität des Benutzers an sowohl dem Client-Terminal **200** als auch dem Anwendungsserver **202**.

[0061] Es wird nun eine beispielhafte bevorzugt Ausführungsform unter Verwendung eines Dreiwege-Authentifizierungsprotokolls und eines Einmal-Passworts als eine Hash-Zeichencodierfolge unter Bezugnahme auf Fig. 3 beschrieben:

- Der Webbrowser **210** des Client-Terminals **200** greift auf die entsprechende Webschnittstelle **214** des Anwendungsservers **202** mit einer Anforderung zum Zugriff auf den Anwendungsprozess **216** zu.
- Die Webschnittstelle **214** des Anwendungsservers **202** spricht mit einer LOG-IN-Bildschirminformation und damit in Verbindung stehenden Instruktionen zum Zugriff auf den Anwendungsprozess **216** an.
- Der Client-Terminal **200** weist den ISO-Prozessor **112** an, den Sicherheitsprozessor **114** zu aktivieren.
- Der ISO-Prozessor **112** löst den Sicherheitsprozessor **114** aus.
- Der Sicherheitsprozessor **114** wartet auf Fingerabdruckdaten von dem Fingerabdrucksensor **110**, und wenn gültige Daten empfangen sind, extrahiert er ein digitales Fingerabdruckmuster, das dann über den ISO-Prozesser **112** an den Webbrowser **210** geliefert wird.
- Der Webbrowser **210** sendet eine verschlüsselte Version des extrahierten Fingerabdruckmusters an den Authentifizierungsserver **204** begleitet mit (oder verschlüsselt mit) damit in Verbindung stehender Information über die betreffende Karte **100'** und den Kartenleser **208**, wie beispielsweise User-ID, IP-Adresse des Client-Terminal **200** und/oder einem hartverdrahteten ID-Code (MAC-Adresse) des Sensors **110**.
- Die Webschnittstelle **220** des Authentifizierungsservers **204** leitet bei Empfang des extrahierten Fingerabdruckmusters zusammen mit der anderen Information von dem Client-Terminal **200** diese Information an den Fingerabdruckübereinstimmungsprozessor **222**.
- Gesteuert durch die Übereinstimmungssoftware **224** verwendet der Fingerabdruckübereinstimmungsprozessor **222** die empfangene User-ID oder andere user- bzw. benutzerspezifische, damit in Verbindung stehende Information, um ein entsprechendes Referenzfingerabdruckmuster von der Datenbank **226** zu erhalten, und vergleicht das genommene Fingerabdruckmuster mit dem Referenz-Fingerabdruckmuster.
- Das Ergebnis (übereinstimmend oder nicht übereinstimmend) wird in einer Zugriffsverlaufsaufzeichnung zusammen mit der damit in Verbindung stehenden Information, die den Terminal **200**, die User-ID-Karte **100'** und die anfordernde Anwendung **216** identifiziert, gespeichert, und die Steuerung geht an die Authentifizierungsserverwebschnittstelle **220** zurück.
- Wenn das Ergebnis übereinstimmt, dann erzeugt die Authentifizierungsserverwebschnittstelle **220** ein Einmal-Passwort in der Form einer Abfragezeichenfolge, die an den Client-Terminal **200** übertragen wird, und verwendet diese Abfragezeichenfolge als einen Hash-Code, um die damit in Verbindung stehende Information, die diese sichert, als die entsprechende Abfrageantwort für mögliche zukünftige Referenz zu verschlüsseln.
- Der Client-Terminal **200** verwendet die empfangene Abfragezeichenfolge als einen Hash-Code, um eine vorher gespeicherte, nicht verschlüsselte Kopie der eingereichten damit in Verbindung stehenden Information zu verschlüsseln, der diese anschließend an die Webschnittstelle **214** des Anwendungsservers **202** als Teil seiner Antwort auf den Anwendungs-Log-In-Prozess sendet.
- Die Webschnittstelle **214** des Anwendungsservers **202** leitet bei Empfang der hash-umgewandelten, damit in Verbindung stehenden Information diese an den Anwendungsdienst **216** weiter, der diese mit einem weitergehenden Log-On-Versuch von diesem Client-Server in Verbindung bringt und zum Zwecke der Bestätigung des übereinstimmenden Ergebnisses die empfangene damit in Verbindung stehende Information weiterlei-

tet, die durch den Client-Terminal unter Verwendung der Abfragefolge hash-bearbeitet wurde, die von dem Authentifizierungsserver als Abfrageantwort vorgesehen wurde.

• Die Webschnittstelle **220** des Authentifizierungsservers **204** leitet bei Empfang der Abfrageantwort von dem Anwendungsserver diese Antwort an den Authentifizierungsprozess **222**, der diese mit der vorher gespeicherten Referenzkopie der erwarteten Abfrageantwort vergleicht, um zu bestimmen, ob die Identität des Benutzers tatsächlich authentifiziert worden ist.

• Eine authentifizierte Benutzeridentitätsinformation, die aus diesem Vergleich resultiert, wird dann an den Anwendungsprozess **216** über die Authentifizierungsserverwebschnittstelle **220** und die Validierungsschnittstelle **218** des Anwendungsservers **202** rückgeführt.

• Die Validierungsschnittstelle **218** verwendet die Authentifizierung, um zu bestätigen, dass die Identität des Benutzers, wie hergestellt, in dem ursprünglichen Log-On-Versuch validiert worden ist.

• Sobald die Identität des Benutzers bestätigt worden ist, fährt der Authentifizierungsprozess **216** dann fort, um direkt mit dem Webbrowser **210** des Client-Anschlusses **200** über die Webschnittstelle **214** des Anwendungsservers **202** in Verbindung zu treten.

[0062] Fig. 6 zeigt einen alternativen Authentifizierungsprozess, bei dem die gesamte Übereinstimmung auf der ISO-kompatiblen Karte von Fig. 4 durch die Sicherheits-CPU **114** ausgeführt wird, und kein externer Authentifizierungsserver **204** verwendet wird. Die linke Seite von Fig. 6 zeigt die Funktionen, die von dem Anwendungsserver **202** ausgeführt werden, während die rechte Seite die Funktionen zeigt, die von der ISO-Chipkarte **100** ausgeführt werden.

[0063] Wenn eine Chipkarte **100** in den Kartenleser **208** eingesetzt wird, wird ein Rückstellsignal RST von dem Kartenleser an sowohl die ISO-CPU (START-Block **502**) als auch die Fingerabdruck-CPU **114** (Fingerabdruckverifikationsblock **504**) gesendet, und beide erhalten Strom VCC von dem Kartenleser **208**. Die ISO-CPU antwortet dann mit der ATR-(Answer-to-Reset)-Nachricht an und kommuniziert PPS (Protocol and Parameters Selection) nach Bedarf (Block **506**). Gleichzeitig geht die Fingerabdruck-CPU in den Wartezustand zum Empfangen von Fingerabdruckdaten, und wenn Daten von dem Sensor **110** empfangen werden, führt diese den Authentifizierungsprozess durch (Block **504**).

[0064] Wenn eine anfängliche Anforderungsanweisung von der Anwendung **216** an die ISO-CPU **112** (Block **508**) gesendet wird, fragt die ISO-CPU (Block **510**) die Sicherheits-CPU über den Authentifizierungsstatus ab. Wenn die Antwort positiv ist, spricht die ISO-CPU auf die Anwendung durch Ausführen der angeforderten Anweisung (Block **512**) an. Ansonsten (entweder eine Fehlernachricht oder keine Antwort von der Sicherheits-CPU **114**) macht sie keine Antwort auf die angeforderte Anweisung sondern wartet vielmehr auf eine neue erste Anforderung (Block **508b**).

[0065] Angenommen, dass der Fingerabdruck verifiziert wurde und die erste Antwort in einer zeitigen Art und Weise empfangen wurde und bestimmt wurde, dass die Anwendung **216** darauf reagieren kann (Block **514**), wird der Anforderungs-/Antwortprozess solange fortgesetzt (Blöcke **516**, **518**, **520**), bis ein vorbestimmter Verifikationszeitablauf überschritten worden ist, während dem keine Anforderungen von der Anwendung empfangen wurden (Block **522**) oder die Anwendung keine erwartete Antwort empfangen hat (Block **524**).

[0066] Fig. 7 ist ähnlich dem Flussschaubild von Fig. 6, jedoch zur Verwendung mit der beispielhaften Karte mit biometrischer Verifikation von Fig. 5 modifiziert. Die ganz linke Seite von Fig. 7 zeigt die Funktionen, die von dem Anwendungsserver **202** ausgeführt werden, die nächste Spalte entspricht dem Leser **208**, die nächste Spalte zeigt die ISO-Kontakte **108**, die nächste Spalte zeigt Funktionen, die von der Sicherheits-CPU **114** ausgeführt werden, während die ganz rechte Seite die Funktionen anzeigt, die von einer nicht modifizierten ISO-Chipkarten-CPU **112** ausgeführt werden.

• Wenn entweder eine Chipkarte in einen Kartenleser eingesetzt wird oder die Anwendungssoftware einen Betrieb der Kartenlesevorrichtung beginnt, wird ein Rückstellsignal **550** von dem Kartenleser **208** an die Sicherheits-CPU **114** gesendet.

• Bald nachdem die Sicherheits-CPU ein Rückstellsignal **550** empfängt, sendet diese ein entsprechendes Rückstellsignal **552** an die ISO-CPU **112**. Gleichzeitig wartet die Sicherheits-CPU Fingerabdruckdaten von dem Fingerabdrucksensor ab.

• Bei Empfang eines Rückstellsignals **552** macht die ISO-CPU eine ATR-(Answer-to-Reset)-Antwort **554** und kommuniziert danach PPS (Protocol and Parameters Selection) nach Bedarf.

• Sobald die Sicherheits-CPU r114 ATR (Answer-to-Reset) von der ISO-CPU empfängt, überträgt sie diese an den Kartenleser (Block **556**) mit zugehörigen PPS-Anweisungen.

• In der Zwischenzeit führt, wenn die Sicherheits-CPU Fingerabdruckdaten empfängt, diese den vorher beschriebenen Authentifizierungsprozess durch. In dem Falle, dass die Authentifizierungsprüfung in einem "DURCHLASS" resultiert, wird der Durchlassstatus für eine festgelegte Zeitdauer beibehalten. Wenn das Ergebnis AUSFALL ist, wartet die Sicherheits-CPU **114** auf neue Fin-

gerabdruckdaten.

• Bei der Anwendungsausführung wird eine Anweisungsanforderung **558** an die Sicherheits-CPU gesendet, die eine Anweisungsanforderung **560** an die ISO-CPU überträgt und auch ihre korrekte Antwort **562** an den Kartenleser überträgt, und zwar nur dann, wenn die Sicherheits-CPU immer noch in dem vorher erwähnten DURCHLASS-Zustand ist oder wenn die letzte korrekte Antwort einen Mehrdaten-Bit-Satz besaß (Testblock **564**).

• Ansonsten (Nein-Zweig **566**) erzeugt die Fingerabdruck-CPU eine Dummyanforderung **568** und überträgt diese an die ISO-CPU und überträgt auch die resultierende ERR-Antwort **570** an den Kartenlesser **216**, wodurch eine richtige Synchronisierung zwischen den Sequenznummern in den Anforderungen und Antworten beibehalten wird.

Verschlüsselung und Sicherheit

[0067] Vor einer Übertragung über ein externes Netzwerk werden sensitive Daten und/oder das Authentifizierungsergebnis bevorzugt möglicherweise unter Verwendung von DES oder Two-Fish-Verschlüsselung verschlüsselt. Der Verschlüsselungsschlüssel kann auf genommenen oder gespeicherten Fingerabdruckdaten, dem User-ID-Code, einem einzigartig zugewiesenen Code des Sensors, der Speicheradresse, benachbarter Daten in dem Speicher, anderen funktionell damit in Verbindung stehenden Daten, einer vorhergehenden Konversation (Transaktion), IP-Adresse, Terminalcode oder einem zugewiesenen Passwort basieren. Alternativ dazu können die sensitiven Daten über das Internet unter Verwendung des sicheren HTTPS-Protokolls gesendet werden.

[0068] Um eine noch größere Sicherheit vorzusehen, kann ein virtuelles privates Gateway (Virtual Private Gateway), wie beispielsweise eine Hardware-DES-Verschlüsselung und -Entschlüsselung, zwischen den sicheren Fingerabdruckauthentifizierungsserver und die Netzwerkverbindung und dementsprechend zwischen den Anwendungsdienstserver und die Netzwerkverbindung eingesetzt werden. Durch eine solche Verwendung eines derartigen virtuellen Gateways oder virtuellen privaten Netzwerks (Virtual Private Network oder "VPN") werden die sensitiven Daten zusätzlich durch eine zusätzliche Verschlüsselungsschicht beispielsweise sowohl DES **128** (typischerweise in dem VPN verwendet) und RSA (durch HTTPS verwendet) geschützt.

[0069] Für speziell sichere Anwendungen können die gesamten Kommunikationen mit zusätzlichen Sicherheitsschichten umwickelt werden. Insbesondere können Nachrichtenköpfe bzw. -kopfsätze in einer unteren Schicht in einer oberen Schicht verschlüsselt sein.

Drahtlose Verbindung

[0070] Andere Ausführungsformen können eine doppelte Schnittstelle für sowohl Kontakt-(ISO 7816) als auch drahtlosen (ISO 1443 A oder B) Betrieb umfassen und bevorzugt eine Leistungseinheit mit mehreren Schnittstellen enthalten, die eine Interoperabilität unter ISO 7816-Kontakt-, ISO 1443 A, ISO 1443 B, ISO 15693 und HID-Legacy-Drahtlossystemen (unter anderem) alle auf einer Karte erlaubt. Alternativ dazu kann die Karte eine Vorkehrung für andere drahtlose Kommunikationstechnologien vorsehen, wie beispielsweise Bluetooth (kurzer Bereich) oder zellulär (mittlerer Bereich) oder Mikrowelle (langer Bereich).

[0071] In Fig. 8 ist eine Chipkarte mit einer biometrischen On-Board-Verifikation gezeigt, die mit einem lokalen Terminal entweder drahtlos oder mittels eines elektrischen Verbinders verbunden sein kann. Größtenteils ist sie hinsichtlich des Aufbaus und der Architektur ähnlich der vorher beschriebenen Ausführungsform von Fig. 1, und gleiche Bezugszeichen (möglicherweise unterschieden durch Anführungszeichen) bezeichnen gleiche Elemente. Insbesondere ist die ISO-CPU **112** an einem anderen Ort gezeigt (unterhalb eher einer Seite von Kontakten **108**), besitzt jedoch eine ähnliche Funktionalität wie zuvor beschrieben.

[0072] Eine ISO-Antenne **132** umfasst zwei Schleifen, die allgemein um den Umfang der Karte **100** angeordnet sind, und sieht eine ISO-kompatible drahtlose Schnittstelle mit der ISO-CPU **112** für sowohl Daten als auch Strom ähnlich der vor, die durch die verdrahtete elektrische Schnittstelle **108** geboten ist. Zusätzlich sieht eine Sicherheitsantenne **134** (bei dem gezeigten Beispiel eine innere Antenne **132** bestehend aus nur einer Schleife) eine separate Stromquelle für die Sicherheits-CPU **114** über einen DC-DC-Leistungsregler **120** vor. Da keine direkte Verbindung für drahtlose Daten mit Ausnahme durch die ISO-CPU **112** besteht, sind die sensitiven Daten, die in der Sicherheits-CPU **114** gespeichert sind, nicht durch eine derartige drahtlose Schnittstelle gefährdet. Alternativ dazu kann, wie vorher bezüglich der Ausführungsformen mit lediglich verdrahteten Verbindungen zu dem externen Leser und dem externen Netzwerk beschrieben wurde, die Funktionalität der beiden Prozessoren kombiniert sein, oder die externe Schnittstelle könnte durch die Sicherheits-CPU **114** anstatt der ISO-CPU **112** vorgesehen sein, in der geeignete drahtlose Sicherheitsmaßnahmen in die somit modifizierte Architektur integriert sein könnten.

[0073] Fig. 9 ist ein Schnitt durch die Karte von Fig. 8. Es sei angemerkt, dass der größte Teil der beschriebenen Komponenten in einem zentralen Kern **126** enthalten ist, wobei sich lediglich Kontaktstellen **108** durch die obere Schutzschicht **122** erstrecken.

Der Schutzbereich des Sensors **110** ist durch ein oberes Fenster in der oberen Lage **122** und ein unteres Fenster in PCB **134** zugänglich, das zwischen der oberen Lage **122** und dem Zentralkern **126** angeordnet ist, und das die erforderlichen elektrischen Verbindungen zwischen den verschiedenen elektronischen Komponenten wie auch einen umgebenden elektrostatischen Entladungsmassekontakt vorsieht, der das aktive Gebiet des Sensors **110** umgibt.

[0074] Auch zu sehen ist eine untere Lage **124** und ein Magnetstreifen **128**.

Fingerabdrucksensor

[0075] Fig. 10 ist ein beispielhaftes schematisches Schaltungsbild für den Sensor **110**, bei dem eine Array **400** aus Sensorzellen **402** in Reihen **404** und Spalten **406** angeordnet ist. Wie gezeigt ist, umfasst jede Zelle **402** ein Aktivierungsgatter **410** und einen Wandler **412**. Ein Fingerabdruck wird durch die Rippen und Täler der Haut an einem Finger gebildet. Jeder Sensorzellenwandler **412** erfährt eine mechanische und/oder elektrische Änderung, wenn eine dieser Rippen die unmittelbare Nähe der Zelle **402** in dem Array **400** berührt, was tatsächlich ein digitales Fingerabdruckbild auf Grundlage von Mikrodruckänderungen über die Sensoroberfläche vorsieht, die durch die Rippen und Täler an der Fingerspitze bewirkt werden. Es sei angemerkt, dass obwohl jeder Wandler **412** als ein einzelner variabler Kondensator gezeigt worden ist, verschiedene Typen von Wandlern existieren, die auf die Anwesenheit von einer dieser Rippen menschlicher Haut ansprechen können: Bei dem bestimmten Beispiel eines drucksensitiven Piezodünnfilmwandlers wird der Film in der Nähe der Zelle verformt und erzeugt eine Ladung, die in einem mit dieser Zelle verbundenen Kondensator gespeichert wird. Die Spannung an dem Kondensator ist somit eine Funktion der mechanischen Spannung, die durch die Verformung des Piezomaterials gebildet wird, was seinerseits eine Funktion darstellt, ob sich ein Berg oder ein Tal über der Zelle befindet. Wenn ein Signal von dem zugeordneten Spaltentreiber **414** das Gatter **410** der Zelle EIN schaltet und der zugeordnete Reihentreiber **416** geerdet ist, erscheint diese Spannung an der Ausgabeleitung **418** der Reihe und wird in ein 8-Bit-Digitalsignal in einem Ausgabetreiber **420** umgewandelt. Zur maximalen Detektion einer Verformung von Piezomaterial kann das elektrische Piezomaterial aus elastischem Material wie beispielsweise Polyimid, geformt sein, oder kann einfach ein elektrisches Polyimid-Piezomaterial sein. Andere beispielhafte Analogwandlertechnologien, die mit einer ähnlichen Arrayorganisation implementiert sein können, umfassen einen variablen Widerstand und eine variable Kapazität. Alternativ dazu könnte jede Zelle aus einem einfachen digitalen Schalter bestehen, der nur ein einzelnes Informationsbit vorsieht. In diesem Fall können zusätzliche Informationsbits durch Bereitstellung mehrerer Zellen in demselben Bereich oder durch Abtasten jeder Zelle mit einer höheren Frequenz erzeugt werden. Eine derartige alternative Ausführungsform vermeidet den Bedarf nach A/D-Wandlern.

[0076] Bei einer beispielhaften Ausführungsform ist der Sensor lediglich 0,33 mm dick und beständig genug, damit er in eine Chipkarte eingebettet werden kann, und wird nicht durch statische Elektrizität, die Elemente oder den Zustand (feucht, trocken, heiß, kalt) der Haut des Benutzers beeinflusst. Eine typische Zelleneinheitsgröße des Sensors **110** beträgt 25 Mikrometer zu 70 Mikrometer und eine typische Teilung beträgt 25 Mikrometer zu 70 Mikrometer. Der beispielhafte Sensor besitzt eine Abtastfläche von 12,5 mm im Quadrat zu 25 mm im Quadrat und ein 8-Bit-Multiempfindlichkeitslevel. Derartige Sensoren können durch ein Array aus TFT (Dünnfilmtransistor) und druckempfindlichem Kondensator hergestellt werden, wie beispielsweise durch ein Dünnfilmpiezomaterial gebildet wird, wie Titanbariumoxid oder Strontiumbariumoxid, und umfasst eine obere Elektrode, die die gesamte Erfassungsfläche bedeckt und schützt. Wenn eine mechanische Spannung angelegt wird, wird eine entsprechende Ladung erzeugt und in dem Dünnfilmpiezokondensator gespeichert. Alternativ dazu kann ein auf Druck basierender Sensor als ein Array aus TFT (Dünnfilmtransistor) zusammen mit dem Dünnfilmkondensator und druckempfindlichen Kondensator hergestellt werden, wie beispielsweise geformt durch eine Lage aus druckleitendem Material, wie beispielsweise Kohlefaser-dispergierter Gummilage, Metall (beispielsweise Kupfer oder Zinn oder Silber), Papier aus Basis plattierter Kohlefaser oder Glasfaser, oder Metall-dispergiertes elastisches Material (wie beispielsweise Silikon), und eine obere Elektrodenlage, die die gesamte Erfassungsfläche bedeckt.

[0077] Reihen- und Spaltentreiber **416**, **414**, deren bestimmtes spezifiziertes Fingerabdrucksensorelement **402** die elektrischen Daten an die Ausgabeschaltung **420** ausgibt, wandeln dadurch die physikalische Eingabe, die für den Fingerabdruck des Benutzers repräsentativ ist, in elektrische Analogdaten um. Ein A/D-Wandler in der Ausgabeschaltung **420** wandelt dann das elektrische Analogsignal in ein elektrisches Digitalsignal um. Jeder Dünnfilmtransistor schaltet selektiv eine geteilte Reihenzwischenverbindung zu der Spannung an ihrem zugeordneten Kondensator, wodurch die Spannung an jedem Kondensator gelesen werden kann und dadurch jede Zellenverformung gemessen werden kann. Eine vollständige Spalte aus Dünnfilmtransistoren wird bevorzugt gleichzeitig geschaltet, und somit kann eine Anzahl von Zellen (beispielsweise 8) in einer gewählten Spalte parallel an verschiedenen Reihenzwischenverbindungen gelesen werden. Die Verbindung mehrerer Gatter als Reihen und Spalten verringert die An-

zahl von Zwischenverbindungen, während das parallele Auslesen mehrerer Zellen von verschiedenen Reihen derselben Spalte die Lesezeit für das gesamte Array verringert. Die Ausgabespannung von dem Sensor kann durch einen Differentialverstärker verstärkt werden. Die Ausgabe eines derartigen Verstärkers kann zur Umwandlung von Analog nach Digital (A/D-Wandler) abgetastet und gehalten werden.

[0078] Das Substrat kann Glas (wie beispielsweise nichtalkalisches Glas), rostfreier Stahl, Aluminium, Keramik (beispielsweise Aluminiumoxid), Papier, Glas-Epoxidharz sein, ist jedoch bevorzugt eine dünne Lage aus kristallinem Silizium. Dünnfilmhalbleitermaterial kann amorphes Silizium, Polysilizium, Diamant oder ein anderer Halbleiterdünnfilm sein. Piezoelektrisches Material kann eine piezoelektrische Keramik sein, wie beispielsweise Blei-Zirkonat-Titanat-(PZT)-Dünnfilme, bevorzugt im Bereich einer Dicke von 0,1 bis 50,0 Mikrometer oder ein piezoelektrisches Poly-mer-Polyimid-Dünnfilmmaterial. Zwischenverbindungsmaterial kann umfassen: Ti/Ni/Cu, Al, Cr/Ni/Au, Ti/Ni/Au, Al/Au, W/Cu, W/Au, W/Au.

[0079] Fig. 11 zeigt einen Trägerzusammenbau für einen Sensor, der auf einem dünnen Substrat aus kristallinem Silizium gebildet ist. Das kristalline Silizium besitzt ausgezeichnete elektrische Eigenschaften und erleichtert eine Integration des Sensorarrays mit den erforderlichen Treiber- und Ausgabeschaltungen, wobei sich jedoch eine relativ große und dünne Lage aus Silikon biegt und bricht, wenn sie einem lokalen Oberflächendruck ausgesetzt wird. Der gezeigte Träger sieht eine wesentlich steifere Struktur vor, als mit einer Lage aus Silizium derselben Gesamtdicke vorgesehen würde.

[0080] Wie gezeigt ist, ist die monolithische Lage aus Silizium **430** etwa 0,1 mm dick und wird durch einen gleichermaßen dicken Rahmen **432** aus Glas-Epoxidharz umgeben, der an einer Verstärkungs- bzw. Montageplatte **434** befestigt ist, die ebenfalls einen Glas-Epoxidharz-Aufbau besitzt und eine Dicke von 0,05 mm aufweist. Der Rahmen **432** und die Montageplatte **434** können leicht unter Verwendung einer herkömmlichen Technologie für gedruckte Leiterplatten (PCB) aufgebaut sein. Insbesondere sind die oberen und unteren Flächen der Montageplatte **434** mit einer dünnen Kupferlage **436** bedeckt, die durch einen Glas-Epoxidharz-Kern getrennt sind. Der Rahmen **432** umfasst eine Anzahl von Lötstellen **440** um seinen äußeren Umfang zur Verbindung mit dem Sicherheitsprozessor **114**. Der dünne Siliziumschip **430** ist über Epoxidharz mit dem Rahmen **432** und der Platte **434** verbunden, und die aktiven Gebiete sind elektrisch mit jeweiligen elektrischen Bahnen in dem Rahmen **430** durch herkömmliche Drahtbondung **442** an den freiliegenden Außenrandabschnitten **444** des Siliziums **430** gekoppelt, das die schützende obere Elektrode **446** umgibt.

Übereinstimmungsalgorithmus

[0081] Zur lokalen On-Board-Verarbeitung, bei der die Verarbeitungsleistung begrenzt ist und lediglich eine einfache 1:1-Übereinstimmung mit einer einzelnen Referenzprobe versucht wird, kann die Fingerabdrucküberein-stimmsoftware auf einem relativ geraden Vergleich von Einzelheiten, die von den beiden Mustern abgeleitet sind, basieren. Beispielsweise kann das Grauskalenbild eines Fingerabdrucks auf zwei Werte verringert werden, nämlich Weiß und Schwarz, und dreidimensionale Rippen werden in zweidimensionale dünne Linien (Vektoren) umgewandelt. Die Genauigkeit des Verfahrens ist daher neben anderen Problemen einer Unschärfe, einem Verschwimmen bzw. Zusammenlaufen, einer Verzerrung, einem teilweisen Fehlen von Liniensegmenten und anderen Effekten ausgesetzt. Obwohl das Einzelheitenverfahren im Prinzip wenig genau ist, erfordert es weniger Berechnungsressourcen und bietet die Möglichkeit einer Kompatibilität mit vielen existierenden Datenbanken.

[0082] Zur Verarbeitung an einem entfernten Authentifizierungsserver ist mehr Verarbeitungsleistung verfügbar und es kann eine genauere Unterscheidung erforderlich sein, beispielsweise ein "POC"-(Phase Only Correlation)-Übereinstimmungsalgorithmus bzw. ein Übereinstimmungsalgorithmus mit phasenbezogener Korrelation. POC ist ein Identifikationsalgorithmus auf Grundlage einer makroskopischen Übereinstimmung ganzer Bilder. POC bringt umgekehrt strukturelle Information über einen breiten Bereich – von Einzelheiten zu dem Gesamtbild, in Übereinstimmung. Daher ist POC in der Lage, eine robuste Genauigkeit gegenüber Rauschen, wie beispielsweise einem Zusammenlaufen wie auch teilweisen Lücken vorzusehen. Im Prinzip ist das POC-Verfahren frei von den nachteiligen Wirkungen einer Positionsverschiebung und Unterschieden in der Helligkeit, ist schnell (etwa 0,1 Sekunden für eine Offlineübereinstimmung) und ist hochgenau. Beispielsweise kann die POC-Software einen Raumfrequenzvergleich der beiden Fingerabdruckmuster unter Verwendung einer zweidimensionalen Fast-Fourier-Transformation ("2DFFT") ausführen. Die 2DFFT wandelt ein Array digitalisierter Daten, die eine physikalische zweidimensionale Verteilung eines Fingerabdrucks darstellen, in einen Frequenzraum, mit anderen Worten eine umgekehrte Raumverteilung um, in der ein höheres Dichtemuster eine höhere Raumfrequenz besitzt. Eine Rotationstransformation kann dazu verwendet werden, die Frequenzraummusterübereinstimmung in Übereinstimmung zu bringen. Die POC-Musterübereinstimmung besitzt den weiteren Vorteil einer Einzelheitenvektorübereinstimmung, da es nicht durch gemeinsame Defekte in dem aufgezeichneten Fingerabdruckmuster fehlgeführt wird, die POC als Rauschen erkennen würde, eine Einzelheitenanalyse jedoch als bedeutsame Daten inter-

pretieren würde.

[0083] Für besonders anspruchsvolle Anwendungen kann eine Hybridmethode eine noch größere Genauigkeit und Sicherheit als jedes Verfahren allein anbieten. Beispielsweise kann eine Einzelheitenvorgehensweise an dem Punkt des Nehmens verwendet werden, während eine POC-Vorgehensweise an einem entfernten Server verwendet werden kann. Als anderes Beispiel kann der Übereinstimmungsprozess sowohl die Einzelheiten als auch die räumlichen Beziehungen analysieren, um eine kombinierte Bewertung zu erzeugen, die die Ergebnisse von beiden in Betracht zieht.

Anwendungen

[0084] Die oben beschriebene Technologie sieht ein hohes Niveau an Sicherheit für mehrere Anwendungen, sowohl kommerziell als auch staatlich, vor. Abhängig von den Anforderungen jeder Anwendung können mehrere sichere Anwendungen nebeneinander existieren und auf derselben Karte und/oder an demselben Authentifizierungsserver funktionieren. Bei einer Ausführungsform kann eine einzelne Karte bis zu 24 unabhängige und sichere Anwendungen enthalten. Beispielsweise wird die Technologie einen Zugriff (physikalisch und/oder logisch) zulassen bzw. verweigern, einen genauen Ort und/oder eine Bewegung von Personal und/oder auf Überwachungslisten geführten Personen bzw. Parteien identifizieren, während gleichzeitig andere sichere Anwendungen jeweils vollständig und sicher isoliert voneinander betrieben werden können.

[0085] Unter den derzeit in Betracht gezogenen Anwendungen sind die folgenden:

- Flughafen-ID/Zugang
- Gebäudesicherheit
- Hotelzimmerzugang und Berechnung
- Krankenhaus
- Online-Spiele
- Downgeloadete Unterhaltung
- Geburtsurkunde
- Computerzugang
- Führerschein – TWIC
- Elektronische Geldbörse
- Notfallmedizinische Information
- Sprengschein
- Zugang zu Regierungs- und Militäreinrichtungen
- HAZMAT-Lizenz
- Gesundheitsfürsorge- & Leistungskarte
- Parkzugang
- Personalausweis
- Pilotenschein
- Hafen-ID/Zugang
- Versicherungsbeweis
- Sozialsicherungskarte
- Trusted Traveler Card
- Visa oder Eintritt/Austritts-Durchlass
- Wählerregistrierungskarte
- Sozialhilfe- & Lebensmittelmarkenkarte

[0086] Für viele dieser Anwendungen sieht der On-Board-Speicher der Karte bevorzugt auch eine sichere Speicherung verschiedener Arten privater persönlicher Information vor, die nur zugänglich ist, wenn der registrierte Kartenhalter seine Identität erwiesen hat und für einen derartigen Zugang autorisiert ist. Beispiele derartiger privater Informationen sind:

- Administrative Information, wie beispielsweise Name, Adresse, Geburtstag, Geburtsort, Nationalität, Religion, Organisationsmitgliedschaften, Sozialsicherheitsnummer, Führerscheinnummer, Personalausweisnummer wie auch Immigrationsinformation, z.B. Visatyp, Visaablauf, Staatszugehörigkeit, etc.
- Finanzielle Information, wie beispielsweise elektronische Geldbörse, Visa, MasterCard, American Express, etc., Kreditkarteninformation, Bankinformation, wie beispielsweise Bankname, Banksaldo, Bankübertragungsinformation, IRS-Nummer, Bankrottaufzeichnungen, Geldübertragungsinformation, etc.
- Physiologische oder Gesundheitsinformation, wie beispielsweise: biometrische Information zur Identifizierung von Personen, wie beispielsweise Größe, Gewicht, Fingerabdruck, Iris, Retina, Handgröße, Knochenstruktur, Stimme, DNA; Bluttyp; medizinische diagnostische Untersuchungsergebnisse; medizinische Vorgeschichte; Medikamentierungen; Versicherungsinformation, psychologische und physiologische Reaktionen auf bestimmte Reize, etc.
- Ereignisinformation, wie beispielsweise Strafaufzeichnungen, Verbrechen, Vergehen, Verletzungen.
- Notfallinformation, wie beispielsweise Friedhof, relative und andere Kontaktinformation, Rechtsanwaltsinformation, religiöse Information.
- Bildung, Arbeitsverlauf, einschließlich Schulbesuch, Grad, Firma, für die gearbeitet wird, bezogen auf FDD.
- Datenzugriffshistorie (speichert die Daten einer Zugriffshistorie in und aus der Karte).
- ID-bezogene Information, wie beispielsweise Fingerabdruckmuster, verarbeitetes Fingerabdruckmuster, Ergebnisse des Fingerabdruckmusters.
- Passwörter wie beispielsweise permanentes Passwort, temporäres Passwort, und/oder Einmalpasswort.
- Verschlüsselungsschlüssel, wie beispielsweise öffentlicher Schlüssel, persönlicher Schlüssel und/oder Einmalschlüssel.

[0087] Es wird nun ein beispielhaftes Karteneintragungssystem beschrieben.

[0088] Der Anmelder: füllt eine Anmeldung aus und reicht diese bevorzugt mit einer Fotografie und einem Fingerabdruck ein. Für die meisten Anmelder sollten eine Prüfung ihres Familienbuchs und eine einfache Querprüfung der eingereichten Information mit einer oder mehreren verfügbaren Regierungs- oder kommerziellen Datenbanken ausreichend sein, um die echte Identität des einzelnen herzustellen.

[0089] Nachdem seine Identität so verifiziert worden ist, fährt der Anmelder mit einer Eingabestation fort, bei der Information, die dem Kartenherausgeber notwendig erscheint, auf die Karte geladen wird. Der Anmelder legt seinen Fingerabdruck auf den Sensor auf der Karte. Sobald der Fingerabdruck zufrieden stellend auf dem Sensor angeordnet und auf die Karte geladen ist, erhält das Kärtchen auf der Karte dann einen Stoß Elektrizität, die bestimmte Sicherungen herausbrennt, um zu verhindern, dass irgendjemand diesen bestimmten Bereich der Karte nochmals beschreiben kann. Anschließend wird das kleine Kärtchen abgetrennt bzw. abgeschnitten (ähnlich einer Nabelschnur). An diesem Punkt kann die Karte nur durch den ISO-Kontaktleser oder das drahtlose ISO-System gelesen oder beschrieben werden.

[0090] In dem Fall eines vernetzten Authentifizierungsservers wird ein Teil oder werden die gesamten selben Daten, die auf die Karte geladen sind, auch in verschlüsselter Form an den entfernten Server übertragen, möglicherweise ergänzt mit zusätzlicher Information, die normalerweise nicht auf der Karte gespeichert ist, die aber für bestimmte Hochsicherheitsanwendungen erforderlich sein kann.

Zusammenfassung

[0091] Eine Hochsicherheitsidentifikationskarte umfasst einen On-Board-Speicher zum Speichern biometrischer Daten und einen On-Board-Sensor zum Nehmen originaler biometrischer Daten. Ein On-Board-Prozessor auf der Karte führt einen Übereinstimmungsvorgang aus, um zu verifizieren, dass die genommenen biometrischen Daten mit den lokal gespeicherten biometrischen Daten übereinstimmen. Wenn eine positive Übereinstimmung vorhanden ist, werden Daten von der Karte zur zusätzlichen Verifikation und/oder Weiterverarbeitung übertragen. Bevorzugt ist die Karte ISO-Chipkarten-kompatibel. Bei einer Ausführungsform funktioniert die ISO-Chipkarte als eine Firewall zum Schützen des Sicherheitsprozessors, der zum Speichern und Verarbeiten der geschützten biometrischen Daten verwendet wird, vor einem böswilligen externen Angriff über die ISO-Chipkarten-Schnittstelle. Bei einer anderen Ausführungsform ist der Sicherheitsprozessor zwischen die ISO-Chipkarten-Schnittstelle und einen nicht modifizierten ISO-Chipkarten-Prozessor eingesetzt und blockiert jegliche externen Kommunikationen so lange, bis der Fingerabdruck des Anwenders mit einem vorher registrierten Fingerabdruck in Übereinstimmung gebracht worden ist. Es ist eine Echtzeitrückkopplung vorgesehen, während der Anwender seinen Finger über den Fingerabdrucksensor bringt, wodurch eine optimale Anordnung des Fingers über dem Sensor erleichtert wird. Die Karte kann dazu verwendet werden, eine Kommunikation mit einem Transaktionsnetzwerk zu ermöglichen oder einen physikalischen Zugang in einen sicheren Bereich zu erhalten.

Patentansprüche

1. Intelligente Identifikationskarte mit:
einem On-Board-Speicher zum Speichern von Referenzdaten,
einem On-Board-Sensor zum Nehmen originaler biometrischer Daten,
einem On-Board-Mikroprozessor zum Vergleich der genommenen biometrischen Daten mit entsprechenden gespeicherten Referenzdaten innerhalb einer vorbestimmten Schwelle und zum Erzeugen einer Verifikationsnachricht nur, wenn eine Übereinstimmung innerhalb einer vorbestimmten Schwelle vorhanden ist, und
einem Mittel zum Kommunizieren der Verifikationsnachricht an ein externes Netzwerk.

2. Identifikationskarte nach Anspruch 1, wobei die Verifikationsnachricht zumindest Auszüge von den gespeicherten Referenzdaten umfasst.

3. Identifikationskarte nach Anspruch 2, wobei die Verifikationsnachricht zumindest Auszüge von den genommenen biometrischen Daten umfasst.

4. Identifikationskarte nach Anspruch 3, wobei die Verifikationsnachricht an ein Fernauthentifizierungssystem zur zusätzlichen Verifikation übermittelt wird.

5. Identifikationskarte nach Anspruch 4, wobei das Fernauthentifizierungssystem entfernt gespeicherte Referenzdaten umfasst, die sich von den lokal gespeicherten Referenzdaten unterscheiden.

6. Identifikationskarte nach Anspruch 4, wobei der On-Board-Mikroprozessor einen anderen Übereinstimmungsalgorithmus als den verwendet, der an dem entfernten Authentifizierungssystem verwendet wird.

7. Identifikationskarte nach Anspruch 2, wobei der gesamte Übereinstimmungsprozess von dem On-Board-Prozessor ausgeführt wird und keine der genommenen biometrischen Daten an das Netzwerk übertragen werden.

8. Identifikationskarte nach Anspruch 2, wobei sowohl die original gehaltenen biometrischen Daten

als auch andere "private" Information, die in dem On-Board-Speicher gespeichert ist, nicht für externe Prozesse verfügbar gemacht sind.

9. Identifikationskarte nach Anspruch 2, wobei die Karte ISO-Chipkarten-kompatibel ist.

10. Identifikationskarte nach Anspruch 9, ferner mit einem ISO-Chipkarten-Prozessor.

11. Identifikationskarte nach Anspruch 10, wobei der Sicherheitsprozessor, der zum Speichern und Verarbeiten der geschützten biometrischen Daten verwendet wird, funktionell durch eine Firewall von dem ISO-Chipkarten-Prozessor getrennt ist.

12. Identifikationskarte nach Anspruch 10, wobei alle externen Daten zu und von dem Sicherheitsprozessor durch den ISO-Chipkarten-Prozessor gelangen.

13. Identifikationskarte nach Anspruch 10, wobei alle externen Daten zu und von dem ISO-Chipkarten-Prozessor durch den Sicherheitsprozessor gelangen.

14. Identifikationskarte nach Anspruch 10, wobei der Sicherheitsprozessor eine erste Verbindung, die zum Laden von Daten während eines Ladeprozesses verwendet wird, und eine zweite Verbindung umfasst, die mit einem externen Netzwerk verbunden ist.

15. Identifikationskarte nach Anspruch, wobei die erste Verbindung dauerhaft außer Betrieb ist, nachdem der Ladeprozess beendet worden ist.

16. Identifikationskarte nach Anspruch 10, wobei der Sicherheitsprozessor, der zum Speichern und Verarbeiten der geschützten biometrischen Daten verwendet wird, funktionell durch eine Firewall von dem ISO-Chipkarten-Prozessor getrennt ist.

17. Identifikationskarte nach Anspruch 10, wobei:
die Karte ein oberes Magnetstreifengebiet und ein unteres geprägtes Gebiet umfasst;
der biometrische Sensor ein Fingerabdrucksensor ist, und
der Sicherheitsprozessor, der ISO-Chipkarten-Prozessor und der Fingerabdrucksensor alle in einem mittleren Gebiet zwischen dem oberen Gebiet und dem unteren Gebiet angeordnet sind.

18. Identifikationskarte nach Anspruch 2, wobei die biometrischen Daten Fingerabdruckdaten umfassen und der Sensor ein Fingerabdrucksensor ist, der Daten von einem auf dem Sensor angeordneten Finger des Anwenders nimmt.

19. Identifikationskarte nach Anspruch 18, wobei eine Echtzeitrückkopplung vorgesehen ist, während der Anwender seinen Finger über den Fingerabdrucksensor bringt, wodurch eine optimale Anordnung des Fingers über dem Sensor erleichtert wird.

20. Identifikationskarte nach Anspruch 18, wobei der Übereinstimmungsprozess einen Hybridübereinstimmungsalgorithmus verwendet, der sowohl Einzelheiten als auch räumliche Gesamtbeziehungen in den genommenen biometrischen Daten berücksichtigt.

21. Identifikationskarte nach Anspruch 18, wobei der Fingerabdrucksensor eine Lage aus kristallinem Silizium umfasst, das durch eine Montageplatte getragen ist.

22. Identifikationskarte nach Anspruch 21, wobei die Montageplatte eine Glasepoxidharzlage umfasst, die zwischen zwei Metalllagen geschichtet ist.

23. Identifikationskarte nach Anspruch 18, wobei die Montageplatte durch einen Trägerrahmen verstärkt ist, der die Siliziumlage umgibt.

24. Identifikationskarte nach Anspruch 1, wobei die Karte ferner ein Mittel zum Beschränken der Verwendung der Karte auf einen vorbestimmten Ort umfasst. zumindest einige der genommenen

25. Identifikationskarte nach Anspruch 1, wobei zumindest einige der genommenen biometrischen Daten und der Referenzdaten an einen separaten Authentifizierungsserver zur sicheren Verifikation einer Identität eines Anwenders vor einer Erteilung eines Onlinezugangs zu einem Anwendungsserver zur Verarbeitung sicherer Finanztransaktionen, die diesen Anwender betreffen, übertragen werden.

26. Identifikationskarte nach Anspruch 25, wobei in Ansprechen auf eine Übereinstimmungsanforderung, die zu einem bestimmten Log-On-Versuch an einem bestimmten Anwendungsserver gehört, der eine positive Übereinstimmung an dem Authentifizierungsserver erzeugt, ein sicheres Dreiwege-Authentifizierungsprotokoll ausgeführt wird, bei dem eine Abfragezeichenabfolge von dem Authentifizierungsserver an die Identifikationskarte gesendet wird, die Identifikationskarte dann die Abfragezeichenabfolge und die Übereinstimmungsanforderung verwendet, um eine Abfrageantwort zu erzeugen, die diese dann an den Anwendungsserver führt, der Anwendungsserver dann die Abfrageantwort an den Authentifizierungsserver leitet, der dann verifiziert, ob die Abfrageantwort gültig ist.

27. Identifikationskarte nach Anspruch 1, wobei die Ausgabe von der Karte dazu verwendet wird, einen physikalischen Zugang in einen sicheren Bereich zu erhalten.

28. Identifikationskarte nach Anspruch 27, wobei eine Aufzeichnung erfolgreicher und nicht erfolgreicher Zugriffsversuche auf der Karte gespeichert wird.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

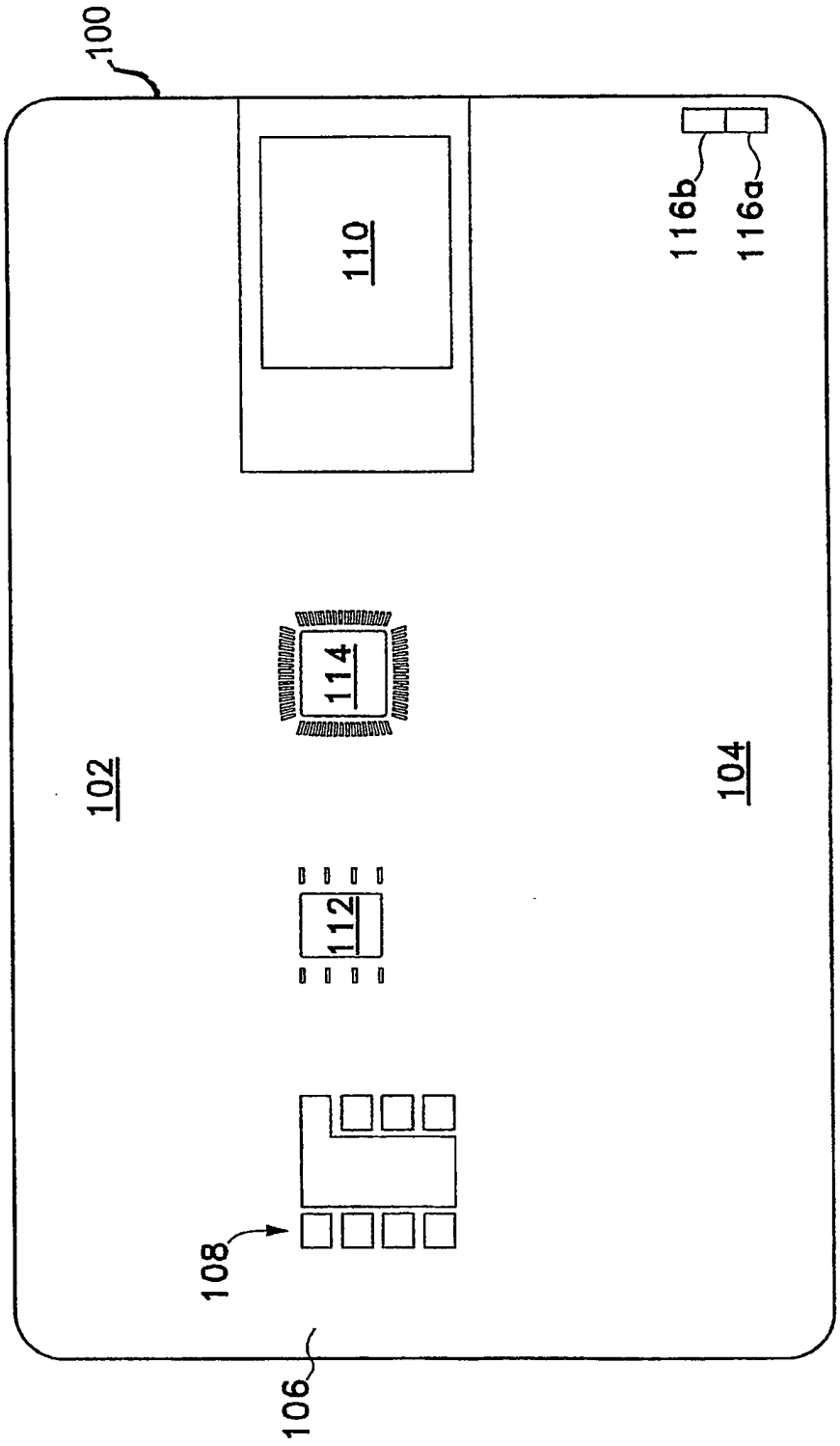


Fig. 1

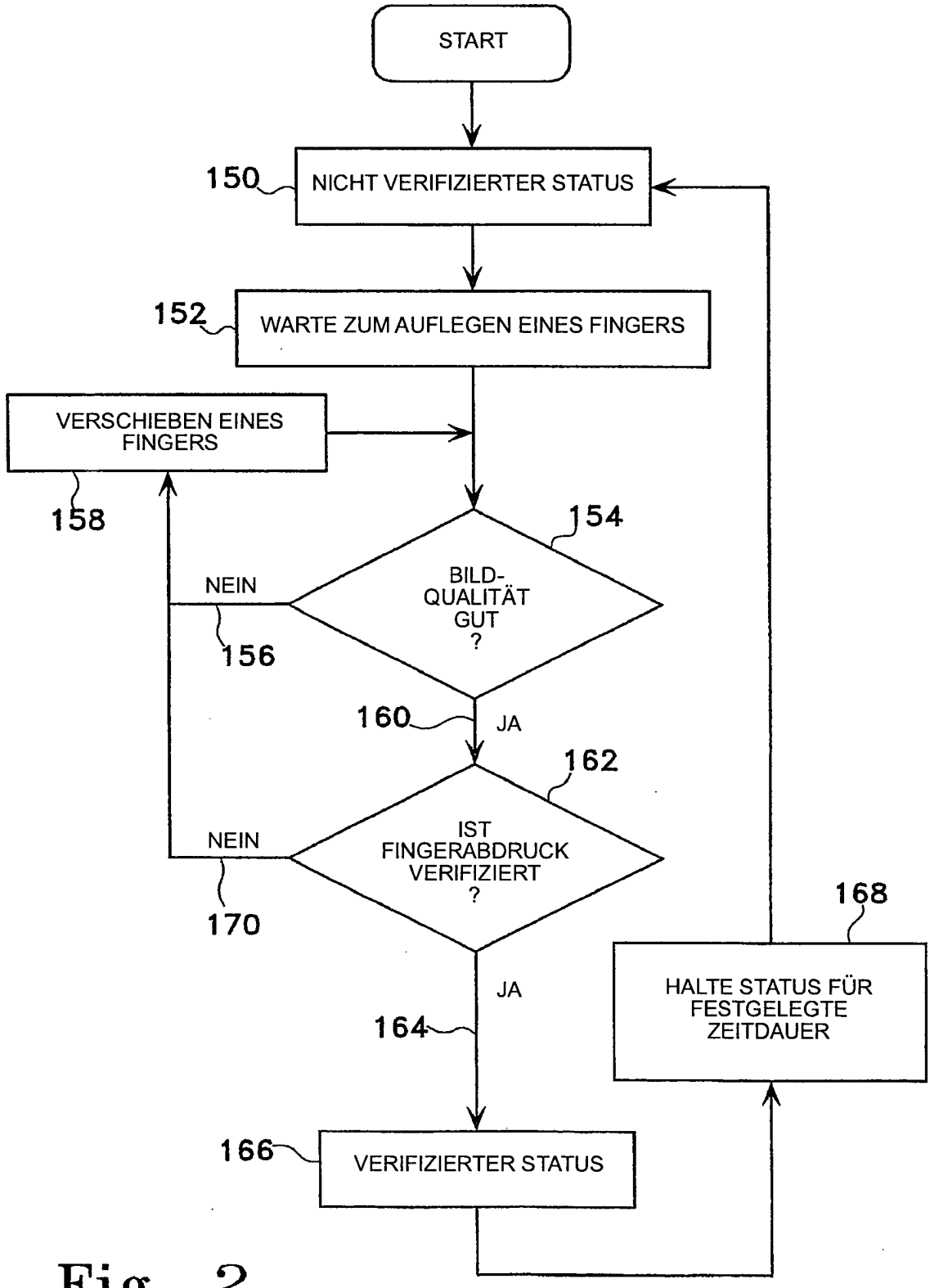

START
150
NICHT VERIFIZIERTER STATUS
152
WARTE ZUM AUFLEGEN EINES FINGERS
VERSCHIEBEN EINES FINGERS
158
154
BILD-QUALITÄT GUT ?
NEIN
156
160
JA
162
IST FINGERABDRUCK VERIFIZIERT ?
NEIN
170
JA
164
168
HALTE STATUS FÜR FESTGELEGTE ZEITDAUER
166
VERIFIZIERTER STATUS

Fig. 2

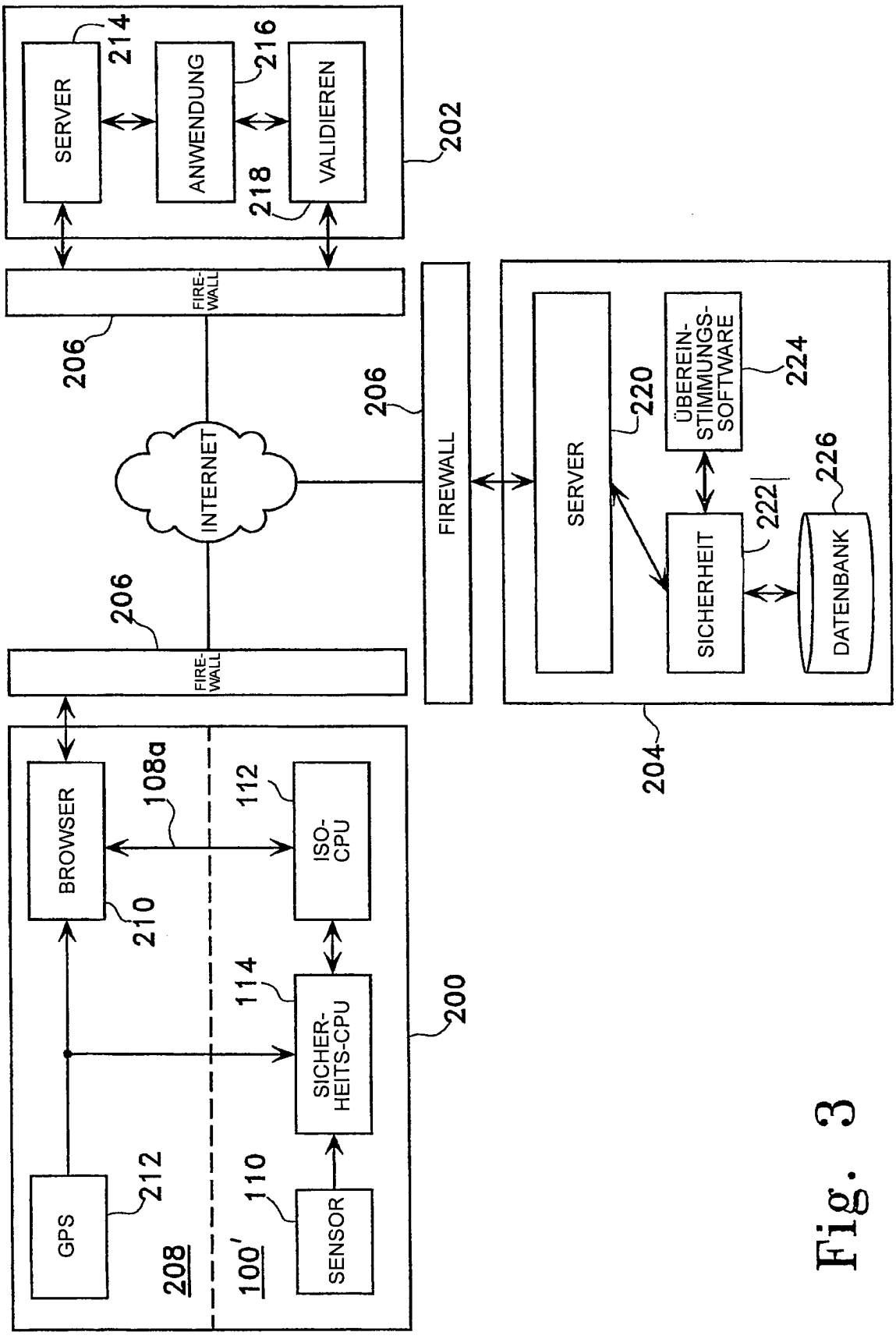

SERVER
214
ANWENDUNG
216
VALIDIEREN
218
202
FIRE-WALL
206
INTERNET
206
FIREWALL
SERVER
220
ÜBEREIN-STIMMUNGS-SOFTWARE
224
SICHERHEIT
222
DATENBANK
226
204
FIRE-WALL
206
BROWSER
108a
112
ISO-CPU
210
114
SICHER-HEITS-CPU
200
GPS
212
208
100'
110
SENSOR

Fig. 3

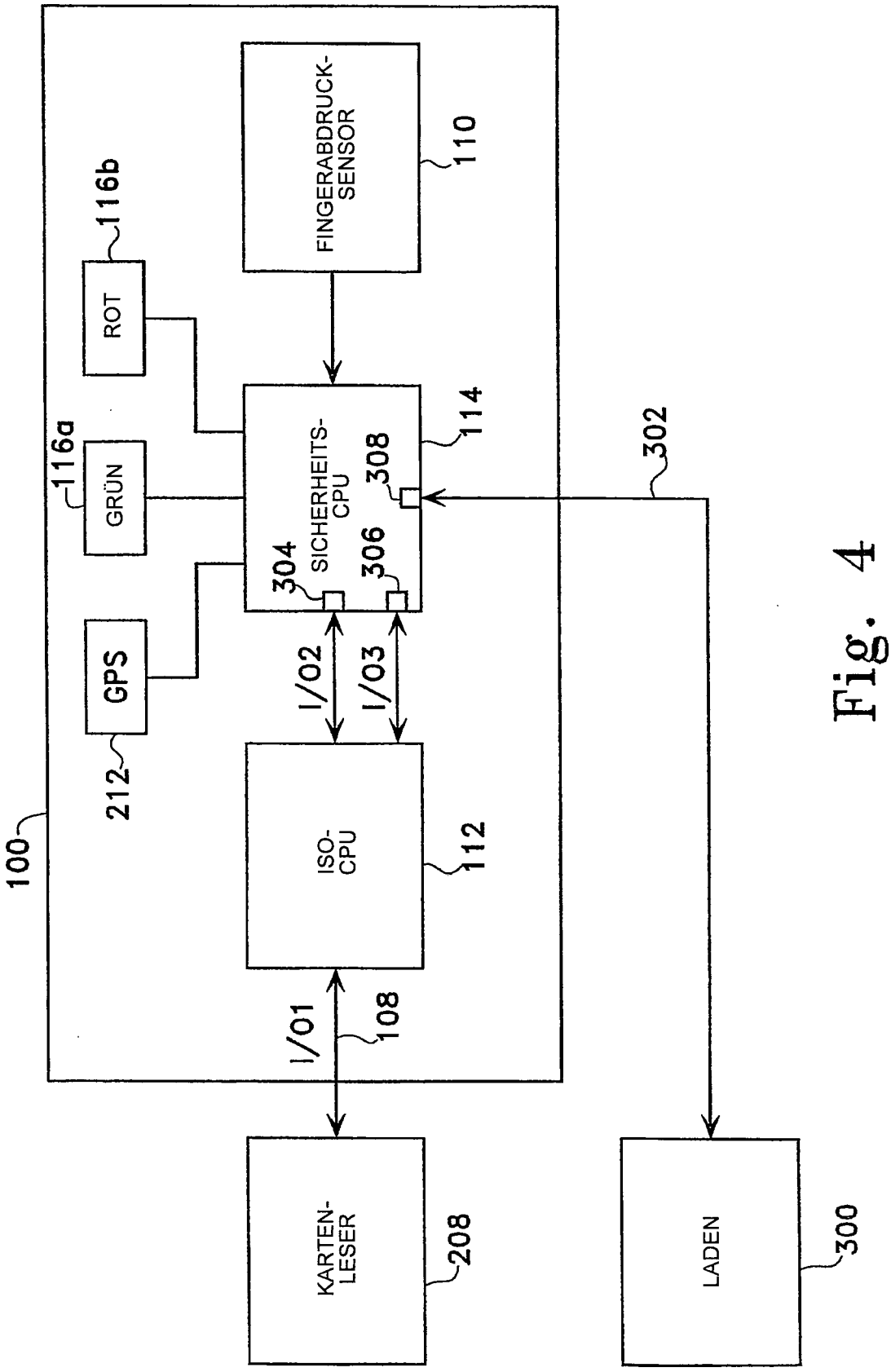

FINGERABDRUCK-SENSOR
110
116b
ROT
116a
GRÜN
GPS
212
100
SICHERHEITS-CPU
114
308
304
306
I/02
I/03
ISO-CPU
112
I/01
108
KARTEN-LESER
208
302
LADEN
300

Fig. 4

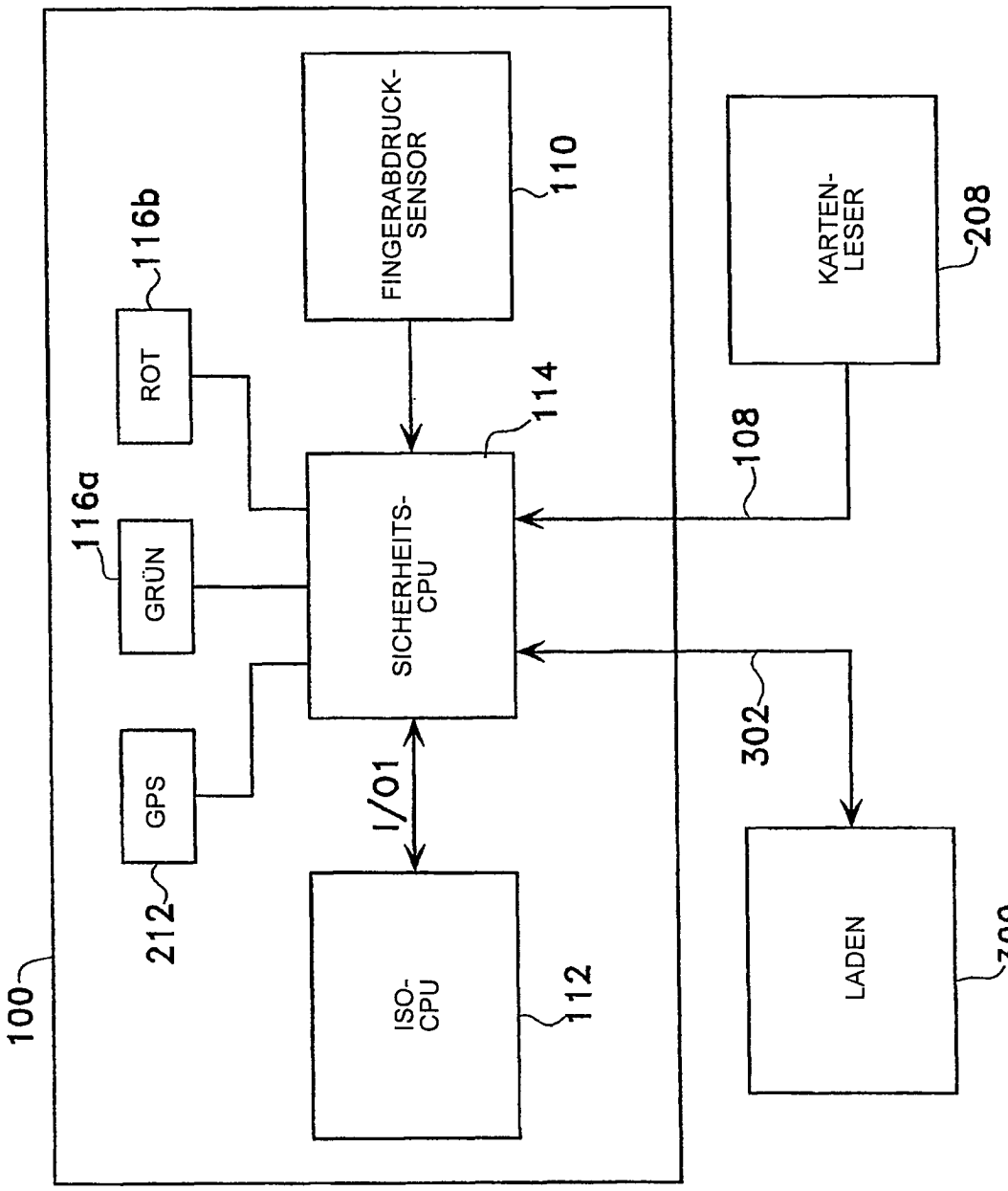

100
FINGERABDRUCK-SENSOR
110
KARTEN-LESER
208
116b
ROT
114
108
116a
GRÜN
SICHERHEITS-CPU
302
I/O1
GPS
212
ISO-CPU
112
LADEN
300

Fig. 5

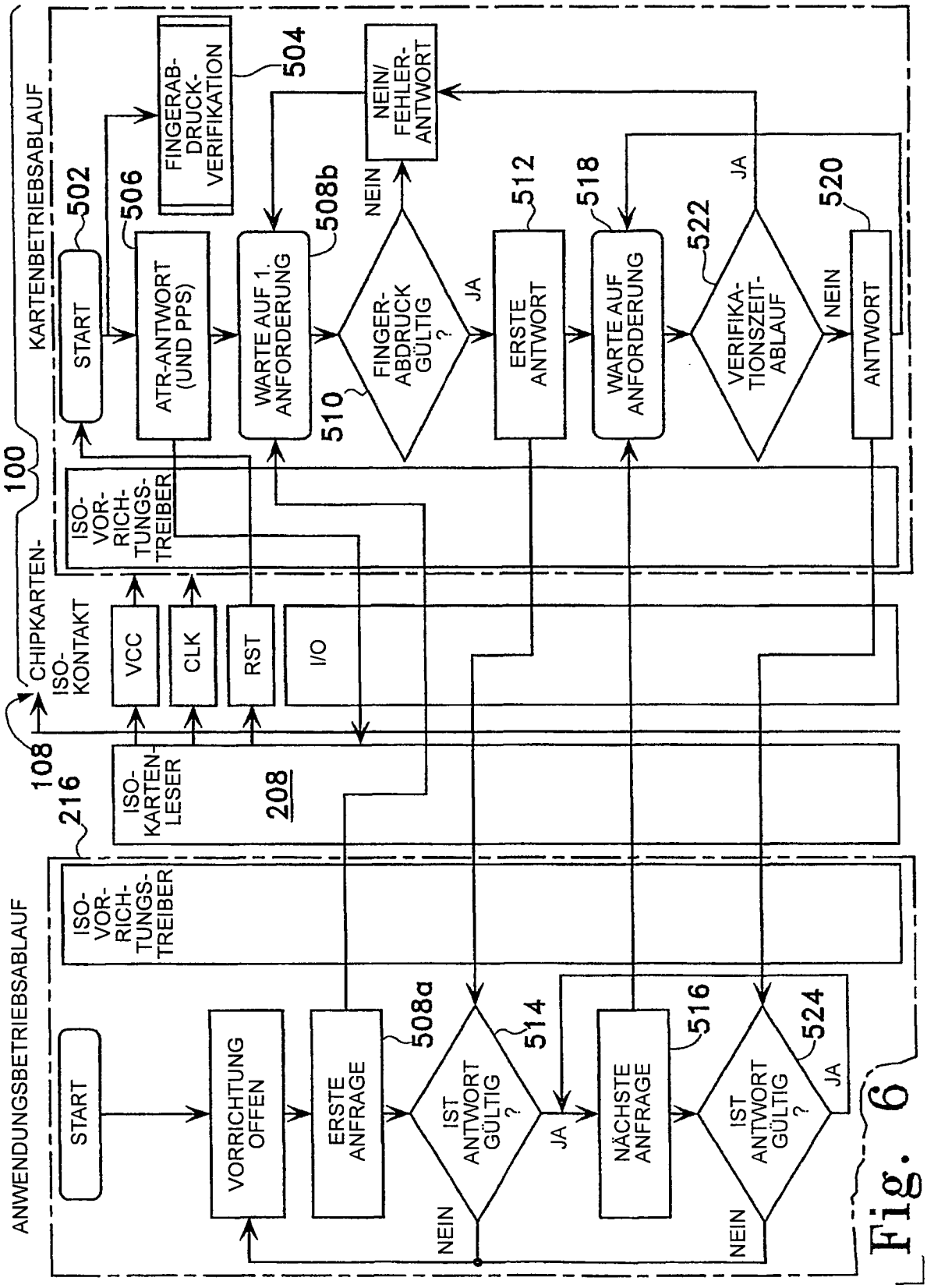

ANWENDUNGSBETRIEBSABLAUF
START
VORRICHTUNG OFFEN
ERSTE ANFRAGE
508a
IST ANTWORT GÜLTIG ?
514
JA
NEIN
NÄCHSTE ANFRAGE
516
IST ANTWORT GÜLTIG ?
524
JA
NEIN
ISO-VOR-RICH-TUNGS-TREIBER
216
ISO-KARTEN-LESER
208
108
CHIPKARTEN-ISO-KONTAKT
VCC
CLK
RST
I/O
100
KARTENBETRIEBSABLAUF
ISO-VOR-RICH-TUNGS-TREIBER
START
502
ATR-ANTWORT (UND PPS)
506
FINGERAB-DRUCK-VERIFIKATION
504
WARTE AUF 1. ANFORDERUNG
508b
510
FINGER-ABDRUCK GÜLTIG ?
NEIN
NEIN/ FEHLER-ANTWORT
JA
ERSTE ANTWORT
512
WARTE AUF ANFORDERUNG
518
VERIFIKA-TIONSZEIT-ABLAUF
522
JA
NEIN
ANTWORT
520

Fig. 6

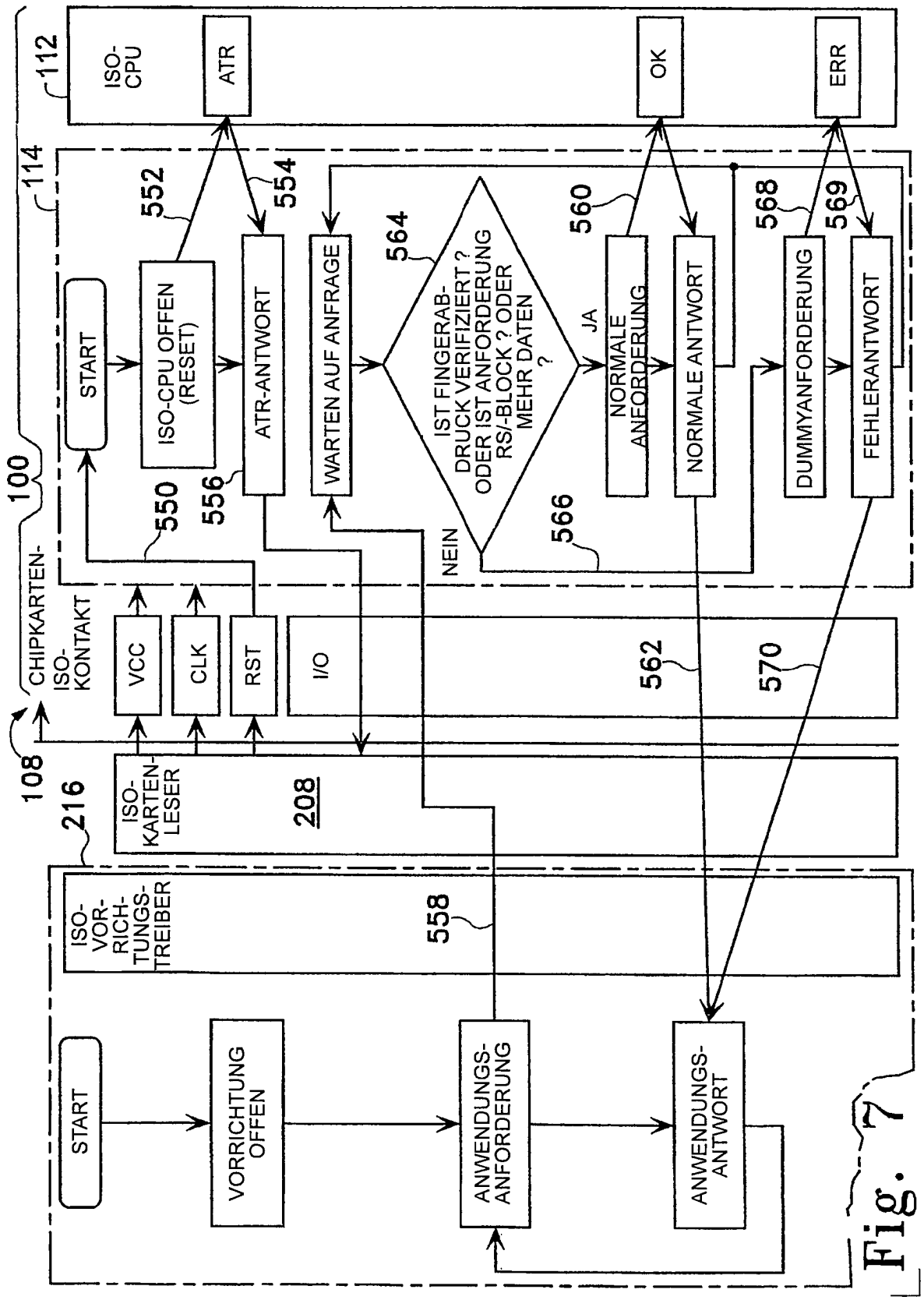

ISO-CPU
112
ATR
OK
ERR
114
552
554
564
560
568
569
START
ISO-CPU OFFEN (RESET)
ATR-ANTWORT
WARTEN AUF ANFRAGE
IST FINGERAB-DRUCK VERIFIZIERT ? ODER IST ANFORDERUNG RS/-BLOCK ? ODER MEHR DATEN ?
JA
NORMALE ANFORDERUNG
NORMALE ANTWORT
DUMMYANFORDERUNG
FEHLERANTWORT
100
CHIPKARTEN-
ISO-KONTAKT
550
556
NEIN
566
VCC
CLK
RST
I/O
562
570
108
216
ISO-KARTEN-LESER
208
ISO-VOR-RICH-TUNGS-TREIBER
558
START
VORRICHTUNG OFFEN
ANWENDUNGS-ANFORDERUNG
ANWENDUNGS-ANTWORT

Fig. 7

Fig. 8

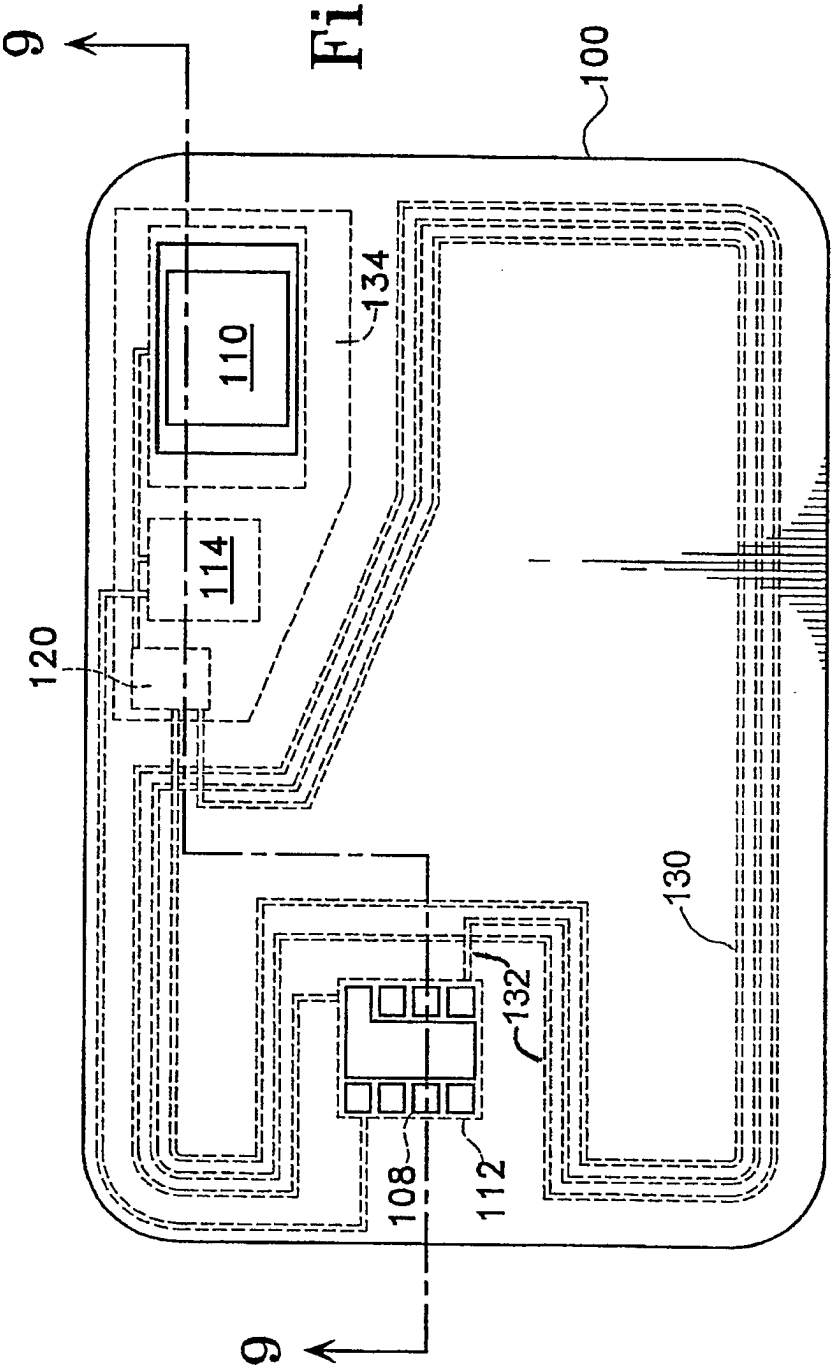
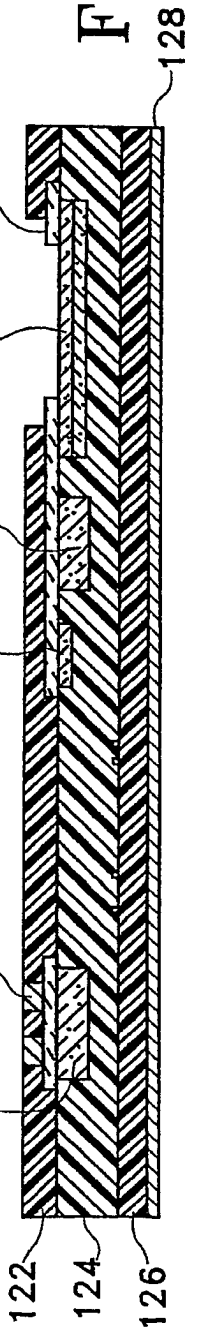

9
100
134
110
114
120
130
132
108
112
9

Fig. 9


128
134
110
114
120
108
112
122
124
126

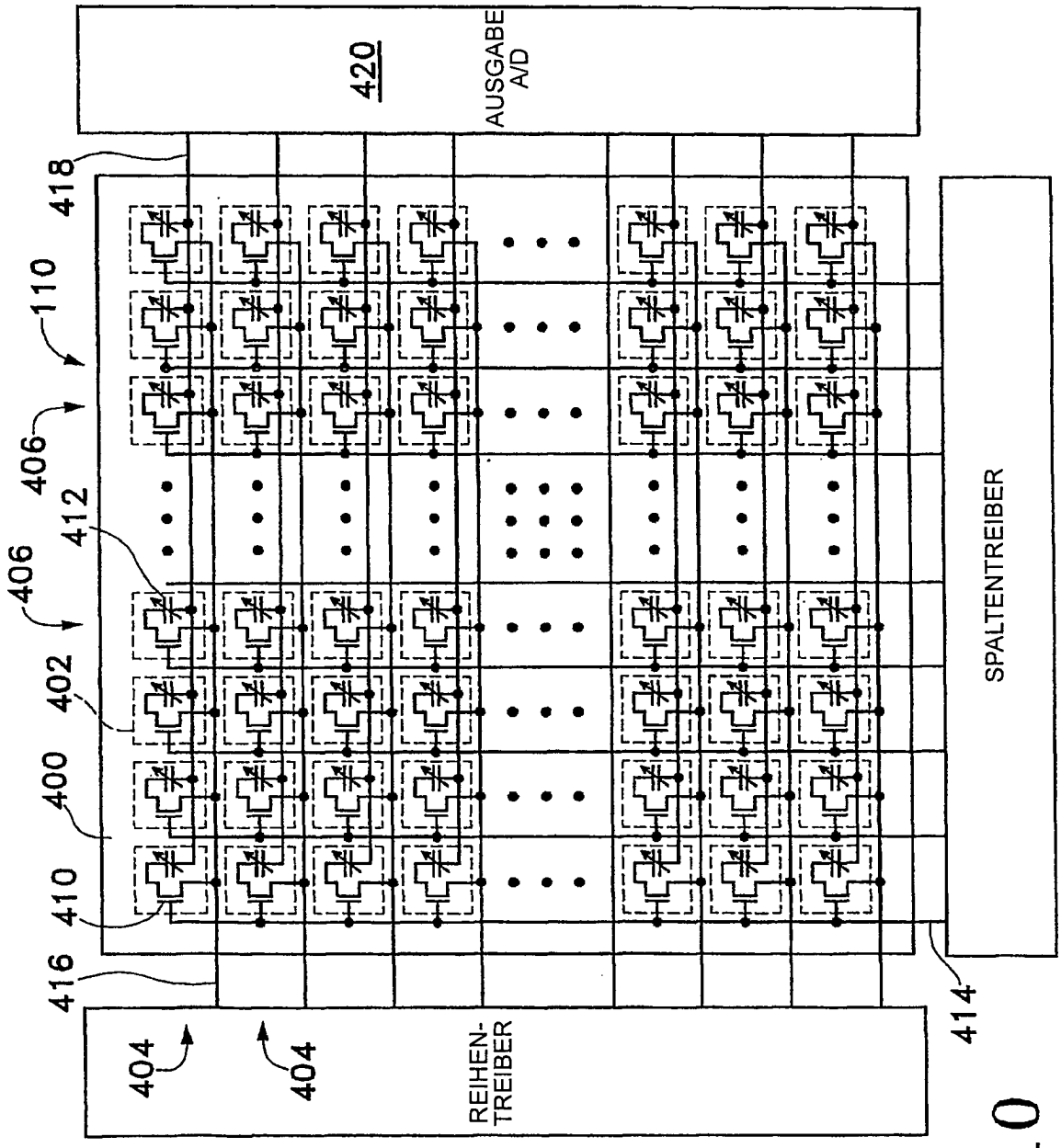

420
AUSGABE A/D
418
110
406
412
406
402
400
410
416
404
404
REIHEN-TREIBER
414
SPALTENTREIBER

Fig. 10

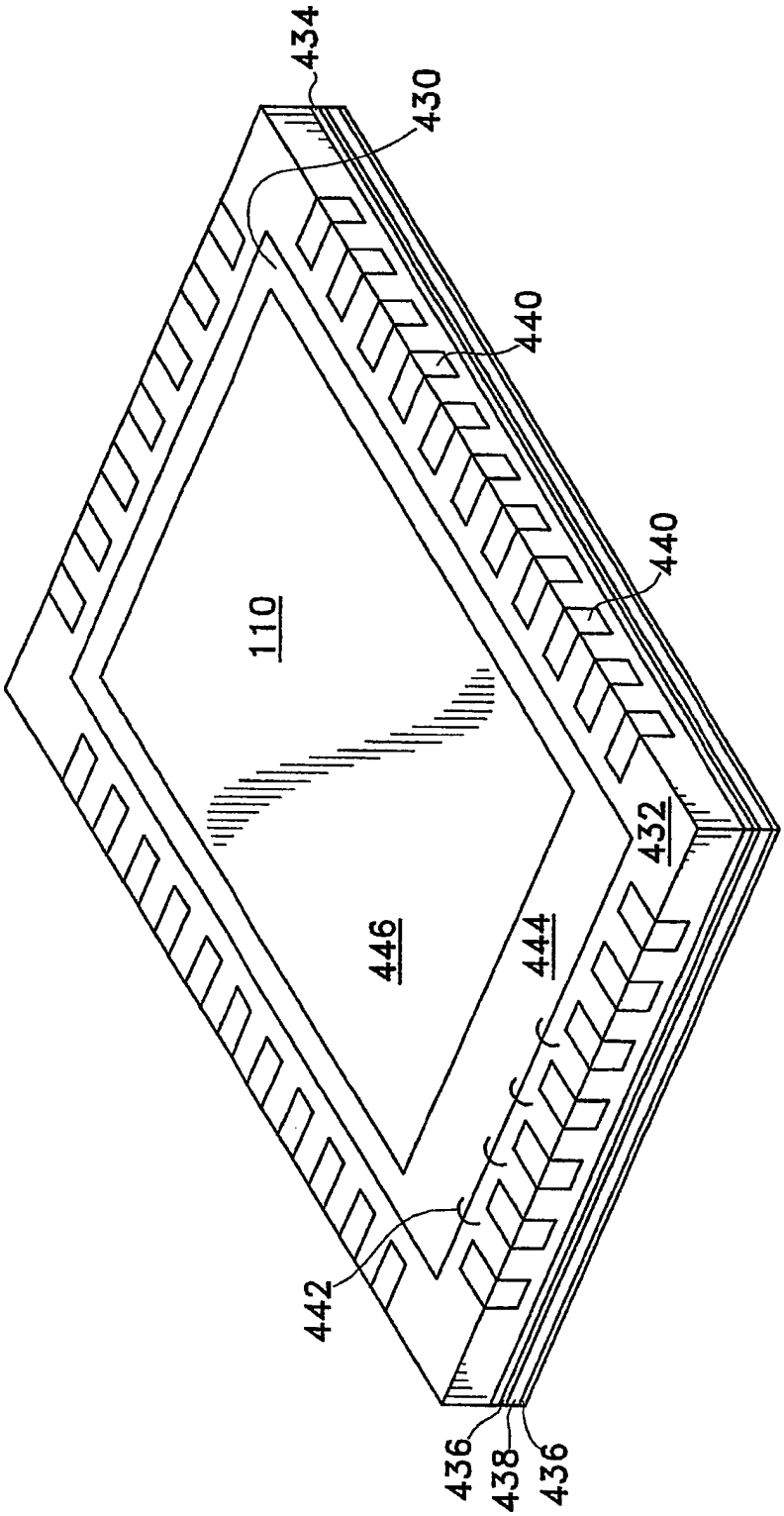


Fig. 11