(19) österreichisches patentamt

(10) **AT 505 459 B1 2009-07-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 982/2007

(22) Anmeldetag: 2007-06-25

(43) Veröffentlicht am: 2009-07-15

(51) Int. Cl.[8]: **G06F 21/06**
H04L 9/10
G06F 12/14

(56) Entgegenhaltungen:
DE 4135767A1 EP 965902A2
JP 2003-208576A US 2003/0005323A1
WO 91/05306A1

(73) Patentinhaber:
TOMSICH PHILIPP DR.
A-1050 WIEN (AT)

(72) Erfinder:
TOMSICH PHILIPP DR.
WIEN (AT)

(54) VERFAHREN ZUR GEWÄHRLEISTUNG EINER SICHEREN KOMMUNIKATION ZWISCHEN EINEM TERMINAL UND DIENSTE-ANBIETERN IN EINEM NETZWERK

(57) Die Erfindung betrifft ein Verfahren zur Gewährleistung einer sicheren Kommunikation zwischen Benutzern zugänglichen Terminals (2) und Anbietern (3) von Diensten in einem Netzwerk (1), wobei zur Kommunikation Prozesse im Terminal (2) und in Netzwerkkomponenten (4) zum Vermitteln bzw. Weiterleiten von Daten in Abhängigkeit von bestimmten gespeicherten Schlüsseln zur Definition von Zugriffsrechten ablaufen sowie ein derartiges Terminal (2). Zur Schaffung einer Sicherheit und der Möglichkeit der Kommunikation mit unterschiedlichen Anbietern (3) mit unterschiedlichen Sicherheitsanforderungen ist vorgesehen, dass jeder Prozess eine Signatur beinhaltet, welche definiert, welche Zugriffsrechte der Prozess besitzt, wobei vor Ablauf jedes Prozesses die jeweilige Signatur und der Schlüssel des Prozesses mit voreingestellten Daten verglichen werden und bei Übereinstimmung der Prozess zugelassen und bei fehlender Übereinstimmung der Prozess gestoppt wird, wobei die Prozesse in sicherheitskritische und sicherheitsunkritische Prozesse getrennt werden und der Ablauf verschiedener Prozesse mit unterschiedlichen Sicherheitsstufen ermöglicht wird, und weiters im Falle einer erkannten Manipulation der Zugriff auf die gespeicherten Schlüssel gesperrt wird, oder die gespeicherten Schlüssel gelöscht werden.

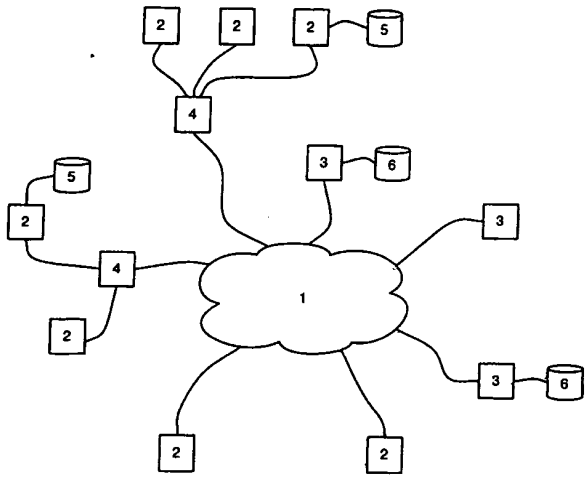

Fig. 1

AT 505 459 B1 2009-07-15

Die Erfindung betrifft ein Verfahren zur Gewährleistung einer sicheren Kommunikation zwischen Benutzern zugänglichen Terminals und Anbietern von Diensten in einem Netzwerk, wobei zur Kommunikation Prozesse im Terminal und in Netzwerkkomponenten zum Vermitteln bzw. Weiterleiten von Daten, wie Router, Firewalls, Proxys oder dgl. in Abhängigkeit von bestimmten gespeicherten Schlüsseln zur Definition von Zugriffsrechten ablaufen, und wobei zumindest ein Teil des Terminals und der Netzwerkkomponenten auf mechanische Manipulation überwacht wird.

Unter den Begriff „Terminal" fallen sämtliche Endgeräte in einem Netzwerk, über die ein Benutzer Prozesse im Netzwerk auslösen kann, wodurch Daten vom Terminal, beispielsweise zu Dienste-Anbietern, gesendet und auch von diesen empfangen werden können. Beispielsweise kann ein Terminal durch ein so genanntes Payment-Terminal gebildet sein, welches in einem Geschäft aufgestellt ist und Benutzern den Zugriff zu Dienste-Anbietern im Netzwerk erlaubt. Häufig ist es erforderlich oder gewünscht, neben den beispielsweise für einen Bezahlvorgang notwendigen Prozessen auch andere Prozesse, wie z.B. zum Zwecke der Werbung, oder auch andere Prozesse auf einem solchen Terminal ablaufen zu lassen. Um die Sicherheit, beispielsweise eines Bezahlvorgangs oder eines Datenaustauschs im Gesundheitswesen, nicht zu gefährden, müssen heutzutage auf Terminals auch andere Prozesse, welche an sich nicht sicher sein müssen, die hohen Sicherheitsanforderungen erfüllen. Dies macht die bestehenden Terminals relativ unflexibel und lässt beispielsweise ein freies Programmieren (und speziell ein Nachladen von Software) nicht zu, da durch eine beliebige, in das Terminal ladbare Software, die Sicherheit anderer Prozesse gefährdet werden könnte.

Neben den bereits genannten Bezahlvorgängen in einem Netzwerk lässt sich das beschriebene Verfahren und das beschriebene Terminal auch im Bereich des Gesundheitswesens, wo eine Sicherheit der Datenübertragung vorausgesetzt wird, ideal einsetzen.

Unter den Begriff „Prozess" fallen sämtliche Vorgänge während der Kommunikation eines Benutzers mit einem Dienste-Anbieter einschließlich dem Versenden und Empfangen von Daten.

Beispielsweise beschreibt die WO 2006/073640 A2 ein Verfahren, welches die Anzeige einer Marke des Bezahlungsnetzes auf einem Bezahl-Terminal am Ende eines Bezahlvorgangs ermöglicht.

Die WO 03/065178 A2 beschreibt ein Verfahren und ein System zur Erzielung verschiedener Dienste über ein Payment-Terminal, welche jedoch eine freie Programmierbarkeit, d.h. ein beliebiges Nachladen von Software, welche die hohen Sicherheitsanforderungen der anderen Anwendungen nicht erfüllt, nicht ermöglicht.

Schließlich zeigt beispielsweise die WO 02/067213 A2 ein Payment-Terminal, welches für mobile Einsätze speziell ausgestaltet ist.

Die US 2003/0005323 A1 bezieht sich auf die Verwaltung bzw. Löschung von sensitiven Daten innerhalb eines Terminals.

Die EP 965 902 A2 beschreibt verschiedene hardwaremäßige Schutzmechanismen.

Die JP 2003-208576 A zeigt ein manipulationssicheres Gerät unter Verwendung von Radiowellen zur Verhinderung des Eindringens von Sonden oder Werkzeugen in das Gehäuse des Geräts. Die Vorrichtung dient zum Schutz von Identifikationsmerkmalen und Schlüsseln.

Viele bekannte Terminals und Verfahren zur Kommunikation zwischen Terminals und Dienste-Anbietern sind trotz der Verwendung von Passworten oder dgl. vor unbenutzten Zugriffen relativ ungeschützt, und bieten insbesondere bei mehreren Anwendungen auf einem Terminal nicht die für bestimmte Anwendungen erforderliche Sicherheit.

Ziel der vorliegenden Erfindung ist daher die Schaffung eines oben genannten Verfahrens durch welche die Sicherheit erhöht werden kann und durch welche eine freie Programmierung des Terminals ermöglicht wird. Nachteile bekannter Verfahren oder Systeme sollen vermieden oder zumindest reduziert werden.

Gelöst wird die erfindungsgemäße Aufgabe dadurch, dass jeder Prozess eine Signatur beinhaltet, welche definiert, welche Zugriffsrechte der Prozess besitzt, wobei vor Ablauf jedes Prozesses die jeweilige Signatur und der Schlüssel des Prozesses mit voreingestellten Daten verglichen werden und bei Übereinstimmung der Prozess zugelassen und bei fehlender Übereinstimmung der Prozess gestoppt wird, wobei die Prozesse in sicherheitskritische und sicherheitsunkritische Prozesse getrennt werden und der Ablauf verschiedener Prozesse mit unterschiedlichen Sicherheitsstufen ermöglicht wird, und weiters im Falle einer erkannten Manipulation der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder die gespeicherten Schlüssel gelöscht werden. Das erfindungemäße Verfahren kombiniert die Software-mäßig implementierte Sicherheit mit der Hardware-implementierten Sicherheit, wodurch die Kommunikation zwischen Benutzern und Dienste-Anbietern in einem Netzwerk, insbesondere im Internet, sicherer gestaltet werden kann. Wesentlich dabei ist, dass sämtliche Prozesse eine Signatur beinhalten und die jeweilige Signatur und der Schlüssel des Prozesses vor der Durchführung des Prozesses überprüft werden, und darüber hinaus die im Terminal gespeicherten Schlüssel dadurch geschützt werden, dass der Teil des Gehäuses des Terminals auf mechanische Manipulation überwacht wird. Weiters überprüft das erfindungsgemäße Verfahren anhand der Signaturen, ob Prozesse überhaupt miteinander kommunizieren dürfen. Beispielsweise wird ein Prozess eines Werbedienst-Anbieters keinen Zugriff auf bestimmte Speicher oder Karten des Terminals erhalten, aber beispielsweise einen Zugriff auf die Anzeige, so dass der Werbedienst-Anbieter bestimmte Informationen an den Benutzer des Terminals weiterleiten kann. Zu diesem Zweck bekommt jede Anwendung bzw. jeder Prozess eine Signatur, welche die Zugriffsrechte des Prozesses definiert. Dies wird Software-mäßig in den unteren Schichten des OSI-Schichten-Modells bewerkstelligt. Durch das erfindungsgemäße Verfahren erfolgt eine Trennung in sichere und nicht sichere Prozesse, wodurch der Zugriff eines Benutzers und Dienste-Anbieter mit unterschiedlichen Sicherheitsstufen im Netzwerk ermöglicht wird. Durch die im Terminal gewährleistete Sicherheit kann es zu keiner Vermischung von Prozessen unterschiedlicher Dienste-Anbieter und somit zu keinen Sicherheitslücken kommen. Das erfindungsgemäße Verfahren stellt einen so genannten technischen Schiedsrichter dar, der über die verschiedenen Sicherheitsniveaus der Dienste-Anbieter wacht.

Wichtig dabei ist, dass die gespeicherten Schlüssel, welche die Zugriffsrechte definieren, in einem sicheren Teil des Terminals untergebracht sind und ein unerkannter Zugriff auf die Schlüssel nicht möglich ist. Im Falle der Erkennung einer Manipulation des sicheren Bereichs des Terminals, werden die gespeicherten Schlüssel entweder gesperrt oder sofort gelöscht, um einen Missbrauch zu verhindern.

Auf diese Weise können auch vermittelnde Geräte im Netzwerk, wie z.B. Router, Firewalls, Proxys oder dgl. sicherer gestaltet werden, indem eine sichere Trennung zwischen administrativen Funktionen und Datenverarbeitung erzielt wird. Beispielsweise können bei einer Firewall die Administration von Firewall-Regeln zugelassen werden, ohne dem Administrator Einblick in tatsächlich stattfindende Kommunikationsflüsse zu geben. Das erfindungsgemäße Verfahren ermöglicht daher die freie Programmierung von Endgeräten oder vermittelnden Komponenten im Netzwerk, ohne die Sicherheit der Kommunikation mit bestimmten Dienste-Anbietern zu gefährden. Dadurch ist eine gute Integrierbarkeit in die Betriebsinfrastruktur von Dienste-Anbietern in den Netzwerken gegeben, die flexible Programmierbarkeit findet unter Wahrung einer informationstechnischen Isolation zwischen den sicherheitskritischen Kernfunktionen (Payment-Kernel, Transaktionen im Rahmen einer Gesundheitsakte und dgl.) und High-Level-Funktionen, die Integration von Mehrwertdiensten und Drittapplikationen erlaubt und Softwaretechnische Erweiterungspunkte enthält, um einen kontrollierten Informationsaustausch zwischen Kernfunktionen und Mehrwertanwendungen zu ermöglichen. Gelöst wird die erfindungs-

gemäße Aufgabe auch durch ein oben genanntes Terminal, wobei eine Einrichtung zur Verwaltung der Zugriffsrechte eine Einrichtung zur Erkennung einer mechanischen Manipulation zumindest an einem Teil des Gehäuses vorgesehen ist, welche Erkennungseinrichtung mit der Verwaltungseinrichtung verbunden ist und bei Erkennung einer Manipulation die Schlüssel sperrbar oder löschbar sind. Durch die Verbindung der erfindungsgemäßen Einrichtung zur Erkennung einer mechanischen Manipulation mit der Einrichtung zur Verwaltung der Zugriffsrechte wird die Sicherheit maßgeblich erhöht und dennoch der Ablauf verschiedener Prozesse an einem Terminal zur Verbindung mit unterschiedlichen Dienste-Anbietern mit unterschiedlichen Sicherheitsstufen ermöglicht.

Vorteilhafterweise ist vorgesehen, dass die Signatur der Prozesse beinhaltet, auf welche Hardware-Einrichtungen, Betriebssystem-Dienste und Dienste im Netzwerk zugegriffen werden darf.

Alternativ oder zusätzlich kann vorgesehen sein, dass die Signatur der Prozesse beinhaltet, auf welche Speicher oder Speicherbereiche zugegriffen werden darf.

Schließlich kann die Signatur der Prozesse auch beinhalten, welche Benutzer zur Kommunikation mit einem Dienste-Anbieter zugelassen werden.

Die Überwachung zumindest eines Teils des Terminals auf mechanische Manipulation kann dadurch erfolgen, dass zumindest ein Teil des Terminals auf akustische Weise auf mechanische Manipulation überwacht wird, indem ein Ultraschall-Signal ausgesendet wird, und das Schallecho des Gehäuses des Terminals detektiert wird und das detektierte Schallecho mit einem gespeicherten Schallecho verglichen wird, und im Fall des Auftretens eines Unterschieds zwischen dem detektierten und dem gespeicherten Schallecho der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder die gespeicherten Schlüssel gelöscht werden. Dies stellt eine sehr effiziente Möglichkeit der Überwachung des Terminals auf mechanische Manipulation hin dar, welche jedoch auch relativ aufwändig ist. Keine mechanische Manipulation am Terminal oder an einem Teil des Terminals bleibt dadurch unerkannt. Das Schallecho des unmanipulierten Gehäuses stellt eine Art Fingerabdruck des Gehäuses dar, der durch eine allfällige Manipulation verändert würde.

Weiters kann eine Spannungsversorgung des Terminals überwacht werden und im Falle einer erkannten Änderung der Spannungsversorgung der Zugriff auf die gespeicherten Schlüssel gesperrt werden oder die gespeicherten Schlüssel gelöscht werden. Dadurch kann verhindert werden, dass das Terminal von unbefugten Personen von der Spannungsversorgung getrennt wird und das Terminal unerkannt zu manipulieren mit dem Ziel, darin gespeicherte Schlüssel in Erfahrung zu bringen. Das selbe gilt natürlich auch für allfällige weitere Spannungsversorgungen, die zur Sicherheit parallel zur Hauptspannungsversorgung des Terminals vorgesehen sein können.

Zur weiteren Erhöhung der Sicherheit kann das erfindungsgemäße Verfahren mit einer Benutzeridentifizierung verknüpft werden. Dabei kann die Identifizierung eines Benutzers des Terminals anhand einer Passworteingabe oder biometrischen Daten, wie Fingerprint, Gesichtsscan, Irisscan oder einer Stimmidentifikation erfolgen.

Um einen Missbrauch der während der Kommunikation zwischen einem Benutzer und einem Dienste-Anbieter verschickten Daten zu verhindern, können die über das Netzwerk gesendeten Daten verschlüsselt und die über das Netzwerk empfangenen Daten im Terminal entschlüsselt werden. Dabei sind verschiedene bekannte Verschlüsselungs- und Entschlüsselungsverfahren anwendbar.

Schließlich kann eine Überwachung der Echtzeit im Terminal erfolgen und im Fehlerfall der Zugriff auf die gespeicherten Schlüssel gesperrt werden, oder die gespeicherten Schlüssel gelöscht werden. Auf diese Weise kann eine Manipulation des Ablaufdatums von Schlüsseln

oder Signaturen der Prozesse wirkungsvoll verhindert werden.

Die Einrichtung zur Erkennung einer mechanischen Manipulation zumindest an einem Teil des Gehäuses, kann durch eine über dem Teil des Gehäuses angeordnete Folie gebildet sein, welche Folie bei mechanischer Manipulation ihre elektrischen Eigenschaften verändert. Beispielsweise kann eine ein feines Drahtnetz enthaltende Folie über die entsprechenden Teile des Gehäuses geklebt werden, wodurch beispielsweise die elektrische Leitfähigkeit der Folie bzw. des Drahtgeflechts bei mechanischer Manipulation verändert und eine Manipulation somit erkannt würde.

Ebenso kann der Manipulationsschutz durch eine Folie aus Polymeren, die ihren Ladungszustand bei Manipulation ändern, gebildet sein.

Alternativ dazu oder auch zusätzlich kann die Erkennungseinrichtung durch einen Ultraschallsender zur Aussendung eines vorgegebenen Signals und einen Ultraschalldetektor zur Detektion des Schallechos des Gehäuses des Terminals gebildet sein, wobei eine Einrichtung zum Vergleich des detektierten Schallechos mit einem gespeicherten Schallecho vorgesehen ist, welche mit dem Schlüsselspeicher verbunden ist, so dass bei Erkennung einer mechanischen Manipulation der Zugriff auf die gespeicherten Schlüssel gesperrt werden kann, oder die gespeicherten Schlüssel gelöscht werden können.

Der Ultraschalldetektor kann dabei durch einen Piezodetektor gebildet sein.

Alternativ dazu oder zusätzlich kann die Erkennungseinrichtung auch durch zumindest eine Lichtquelle und zumindest einen optischen Detektor gebildet sein, die entsprechend angeordnet werden, um eine Manipulation am Teil des Gehäuses des Terminals sicher zu erkennen.

Die Spannungsversorgung des Terminals kann durch einen Anschluss zur Verbindung mit einer externen Spannungsversorgung gebildet sein.

Darüber hinaus kann die Spannungsversorgung eine interne Backup-Batterie umfassen.

In beiden Fällen ist es von Vorteil, wenn eine Einrichtung zur Überwachung der Spannungsversorgung vorgesehen ist, welche mit dem Schlüsselspeicher verbunden ist, so dass bei Erkennung eines Absinkens der Spannung der Spannungsversorgung oder der internen Backup-Batterie unter einem vorgegebenen Grenzwert die gespeicherten Schlüssel gelöscht werden. Diese Maßnahme stellt sicher, dass bei einer ungewollten oder bewusst eingeleiteten Spannungsreduktion ein Zugriff auf die im Gerät gespeicherten Schlüssel unmöglich wird. Nach der Detektion eines Abfalls der Spannung unter einen vorgegebenen Grenzwert muss das Terminal zur Aufbringung neuer Schlüssel entsprechend gewartet werden und ist bis dahin, zumindest für die sicheren Anwendungen, unbrauchbar.

Wie bereits oben erwähnt, können zusätzlich Mittel zur Identifizierung von Benutzern vorgesehen sein. Diese Mittel können durch eine Tastatur zu Eingabe eines Passworts oder verschiedene Biometrie-Sensoren, wie eine Kamera zur Detektion des Gesichts oder eines Teils des Gesichts eines Benutzers oder einen Fingerprint-Sensor oder ein Mikrofon zur Aufnahme der Sprache eines Benutzers gebildet sein.

Zur Vermeidung eines Datenmissbrauchs während der Kommunikation von Benutzern mit Dienste-Anbietern im Netz können im Terminal Mittel zur Verschlüsselung der über das Netzwerk gesendeten Daten und Mittel zur Entschlüsselung der über das Netzwerk empfangenen Daten vorgesehen sein.

Zur Überwachung beispielsweise eines Ablaufdatums von Zertifikaten und somit zur Verhinderung eines diesbezüglichen Missbrauchs, beispielsweise durch Manipulation der Zeit, ist

vorzugsweise ein Echtzeit-Modul vorgesehen. Ein Echtzeit-Modul kann beispielsweise durch einen Funkuhr-Empfänger oder dgl. gebildet sein.

Zur Überprüfung der Berechtigung eines Benutzers kann auch ein Kartenleser oder eine Schnittstelle für einen Kartenleser am Terminal vorgesehen sein.

Der Netzwerkanschluss des Terminals ist vorzugsweise zum Anschluss an ein TCP/IP- (Transmission Control Protocol/Internet Protocol) Netzwerk ausgebildet.

Insbesondere kann der Netzwerkanschluss durch einen Ethernetanschluss gebildet sein.

Das Netzwerk ist vorzugsweise durch das World Wide Web bzw. Internet gebildet.

Die vorliegende Erfindung wird anhand der beigefügten Zeichnungen näher erläutert.

Darin zeigen:

Fig. 1 schematisch ein Blockschaltbild zur Veranschaulichung einer Kommunikation von Benutzern mit Dienste-Anbietern in einem Netzwerk; Fig. 2 ein Blockschaltbild einer Ausführungsform eines erfindungsgemäßen Terminals; und Fig. 3 ein Flussdiagramm zur Veranschaulichung des Verfahrens beim Starten eines Prozesses in einem Terminal der gegenständlichen Art.

Fig. 1 zeigt ein Blockschaltbid eines Netzwerks 1, beispielsweise des Internets, an dem verschiedene Terminals 2 angeschlossen sind, die Benutzern zugänglich sind. Bei derartigen Terminals 2 handelt es sich um Endgeräte, wie z.B. Payment-Terminals, wie sie zur Benutzung von Kunden in Geschäften aufgestellt werden oder zur Bedienung durch Ärzte in Ordinationen oder Spitälern platziert sind. Ziel ist die Kommunikation zwischen einem Terminal 2 und einem Anbieter 3 von Diensten, welche ebenfalls an das Netzwerk 1 angeschlossen sind. Dabei unterscheiden sich verschiedene Dienste-Anbieter üblicherweise durch unterschiedliche Sicherheitsniveaus bzw. Sicherheitslevel, welche im Terminal 2 unterschiedlich behandelt werden müssen. Um beispielsweise die erforderliche Sicherheit bei einem Bezahlvorgang bzw. der Kommunikation mit einer Bank als Dienste-Anbieter 3 zu gewährleisten, müssen auch andere unsichere Dienste-Anbieter, wie z.B. Werbedienste-Anbieter, im Terminal 2 entsprechend behandelt werden, um die Sicherheit der Kommunikation mit dem sicheren Dienste-Anbieter 3 nicht zu gefährden. In Folge dessen wird das nachträgliche Programmieren von unsicheren Applikationen im Terminal 2 sehr aufwändig, da die sichere Kommunikation mit einem Anbieter 3 nicht gefährdet werden darf. Bestehende Terminals 2 sind diesbezüglich sehr unflexibel, weshalb beispielsweise mehrere Terminals 2 für die Kommunikationen mit den verschiedenen Anbietern 3 verwendet werden oder die Integration der Kommunikation mit verschiedenen Anbietern 3 im Terminal 2 in aufwändiger Weise hergestellt wird.

Zusätzlich können Komponenten 4 vorgesehen sein, welche keine Endgeräte, wie die Terminals 2, sind, sondern zum Vermitteln bzw. Weiterleiten von Prozessen dienen. Unter derartige vermittelnde oder weiterleitende Komponenten fallen beispielsweise Router, Firewalls, Proxys oder dgl.. Die Terminals 2 oder Anbieter 3 der Dienste im Netzwerk 1 greifen üblicherweise auf Daten von entsprechenden Datenbanken 5, 6 zu, welche während der Kommunikation im Netzwerk 1 zwischen den Benutzern der Terminals 2 und den Dienste-Anbietern 3 ausgetauscht werden.

Wie bereits oben erwähnt, kann es sich bei den Dienste-Anbietern um Krankenhäuser und Ärzte, welche Daten über Patienten zur Verfügung stellen sowie Werbedienstleistern, die Werbung zur Verfügung stellen oder Apotheken, die Daten über Medikamente und Rezepte zur Verfügung stellen sowie Banken, welche für den Zahlungsverkehr zuständig sind, handeln. Bei der Kommunikation eines Benutzers 2 mit verschiedenen Dienste-Anbietern 3 sind jeweils unterschiedliche Sicherheitsstufen zu beachten.

Fig. 2 zeigt das Blockschaltbild eines erfindungsgemäßen Terminals 2 umfassend ein Gehäuse 10, einen Netzwerkanschluss 11, eine Anzeige 12, Eingabemittel 13, einen Speicher 14 und einen Speicher 15 für Schlüssel zur Definition von Zugriffsrechten von Prozessen. Weiters ist eine Spannungsversorgung 16 vorgesehen, welche durch eine externe Spannungsversorgung 17 gebildet sein kann. Zusätzlich kann eine Backup-Batterie 18 vorgesehen sein. Weiters ist eine Einrichtung 19 zur Verwaltung der Zugriffsrechte vorgesehen und eine Einrichtung zur Erkennung einer mechanischen Manipulation zumindest an einem Teil 21 des Gehäuses 10. Der Teil 21 des Gehäuses 10 wird so gewählt, dass er sämtliche wesentliche Bestandteile enthält, die vor einer Manipulation geschützt werden sollen. Insbesondere zählt dazu der Speicher 15 für die Schlüssel aber auch die zentrale Recheneinheit 22 oder ein Speicher 23, der die Prozesse zum Starten des Terminals 2 enthält. Die Erkennungseinrichtung 20 ist mit der Verwaltungseinrichtung 19 verbunden, so dass bei Erkennung einer Manipulation des Teils 21 des Gehäuses 10 die im Speicher 15 abgelegten Schlüssel gesperrt oder gelöscht werden können. Die Einrichtung 20 zur Erkennung einer mechanischen Manipulation zumindest an einem Teil 21 des Gehäuses 10 ist mit entsprechenden Sensoren 24, wie z.B. akustischen Sensoren, optischen Sensoren oder einer Folie, welche bei mechanischer Manipulation ihre elektrischen Eigenschaften verändert, verbunden.

Weiters kann eine Einrichtung 25 zur Überwachung der Spannungsversorgung 16 vorgesehen sein, welche mit der Erkennungseinrichtung 20 und in der Folge mit der Verwaltungseinrichtung 19 und dem Schlüsselspeicher 15 verbunden ist. Bei Erkennung eines Absinkens der Spannung der Spannungsversorgung 17 oder der internen Backup-Batterie 18 unter einem vorgegebenen Grenzwert können die im Speicher 15 gespeicherten Schlüssel sofort gelöscht werden, um einen Missbrauch bei nicht zur Verfügung stehenden Spannungsversorgungen zu verhindern.

Schließlich können Mittel 26 zur Verschlüsselung und Entschlüsselung der über das Netzwerk 1 gesendeten Daten bzw. über das Netzwerk 1 empfangenen Daten vorgesehen sein. Die Ver- und Entschlüsselungsmittel 26 sind vorzugsweise ebenfalls im sicheren Teil 21 des Gehäuses 10 des Terminals 2 angeordnet.

Um zu verhindern, dass durch Manipulation der Zeit ein Missbrauch der Schlüssel vorgenommen wird, kann ein Echtzeitmodul 27 vorgesehen sein. Über einen Anschluss 28 kann auch ein Kartenleser oder dgl. angeschlossen werden, über den ein Benutzer des Terminals 2 entsprechend identifiziert werden kann. Die Identifizierung eines Benutzers des Terminals 2 kann auch über entsprechende Biometrie-Sensoren (nicht dargestellt) oder die Eingabemittel 14, über welche ein Passwort eingegeben werden kann, realisiert werden.

Fig. 3 zeigt ein Flussdiagramm während der Startsequenz eines Terminals 2, wobei nach dem Aktivieren des Terminals 2 gemäß Schritt 100 in Schritt 101 die entsprechenden Daten im Speicher 23 in die zentrale Recheneinheit 22 (s. Fig. 2) geladen werden. Gemäß Abfrage 102 werden die Signaturen und der Schlüssel des Prozesses mit voreingestellten Daten verglichen und bei Übereinstimmung entsprechend Schritt 103 die Daten allenfalls entschlüsselt und gemäß Schritt 104 der Prozess durchgeführt. Im Fehlerfall, d.h. bei Nichtübereinstimmung der Signaturen und der Schlüssel mit voreingestellten Daten, werden die Schlüssel gemäß Schritt 105 gesperrt oder sogar gelöscht. Dies erfolgt durch die zentrale Recheneinheit 22 in Zusammenhang mit der Verwaltungseinrichtung 19 gemäß der Ausführungsvariante in Fig. 2.

Das erfindungsgemäße Verfahren und das erfindungsgemäße Terminal zeichnen sich durch die gute Integrierbarkeit in die Betriebsinfrastrukturen von Kommunikationsnetzen, durch ihre hohe Sicherheit und ihre flexible Programmierbarkeit unter Wahrung einer informationstechnischen Isolation zwischen sicherheitskritischen Kernfunktionen und sicherheitsunkritischen Funktionen sowie durch eine zentrale und dezentrale Bereitstellung von Inhalten und Mehrwertanwendungen von Dienste-Anbietern sowie eine gesicherte Datenhaltung im Terminal durch entsprechende Verschlüsselungsmechanismen aus. Insbesondere zeichnet sich die vorliegende Erfin-

dung durch eine Sicherung von Angriffen durch mechanische Manipulation aus. Es findet im Terminal 2 eine Kopplung und Verknüpfung der sicherheitskritischen Anwendungen, wie z.B. Bezahlung, und der sicherheitsunkritischen Anwendungen, wie z.B. Werbeeinblendungen, innerhalb eines Terminals 2 unter Sicherstellung einer informationstechnischen Trennung zwischen der Verarbeitung von sicherheitskritischen und -unkritischen Anwendungen statt. Dennoch können Ressourcen gemeinsam genutzt werden.

Patentansprüche:

1. Verfahren zur Gewährleistung einer sicheren Kommunikation zwischen Benutzern zugänglichen Terminals (2) und Anbietern (3) von Diensten in einem Netzwerk (1), wobei zur Kommunikation Prozesse im Terminal (2) und in Netzwerkkomponenten (4) zum Vermitteln bzw. Weiterleiten von Daten, wie Router, Firewalls, Proxys oder dgl. in Abhängigkeit von bestimmten gespeicherten Schlüsseln zur Definition von Zugriffsrechten ablaufen, und wobei zumindest ein Teil des Terminals (2) und der Netzwerkkomponenten (4) auf mechanische Manipulation überwacht wird, *dadurch gekennzeichnet*, dass jeder Prozess eine Signatur beinhaltet, welche definiert, welche Zugriffsrechte der Prozess besitzt, wobei vor Ablauf jedes Prozesses die jeweilige Signatur und der Schlüssel des Prozesses mit voreingestellten Daten verglichen werden und bei Übereinstimmung der Prozess zugelassen und bei fehlender Übereinstimmung der Prozess gestoppt wird, wobei die Prozesse in sicherheitskritische und sicherheitsunkritische Prozesse getrennt werden und der Ablauf verschiedener Prozesse mit unterschiedlichen Sicherheitsstufen ermöglicht wird, und weiters im Falle einer erkannten Manipulation am Terminal (2) oder einer Netzwerkkomponente (4) der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder die gespeicherten Schlüssel gelöscht werden.

2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, dass die Signatur der Prozesse beinhaltet, auf welche Hardwareeinrichtungen, Betriebssystem-Dienste und Dienste im Netzwerk (1) zugegriffen werden darf.

3. Verfahren nach Anspruch 1 oder 2, *dadurch gekennzeichnet*, dass die Signatur der Prozesse beinhaltet, auf welche Speicher oder Speicherbereiche zugegriffen werden darf.

4. Verfahren nach einem der Ansprüche 1 bis 3, *dadurch gekennzeichnet*, dass die Signatur der Prozesse beinhaltet, welche Benutzer zugelassen werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, *dadurch gekennzeichnet*, dass zumindest ein Teil des Terminals (2) auf akustische Weise auf mechanische Manipulation überwacht wird, indem ein Ultraschallsignal ausgesendet wird und das Schallecho des Gehäuses des Terminals (2) detektiert wird und das detektierte Schallecho mit einem gespeicherten Schallecho verglichen wird und dass im Falle des Auftretens eines Unterschieds zwischen dem detektierten und dem gespeicherten Schallecho der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder die gespeicherten Schlüssel gelöscht werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, *dadurch gekennzeichnet*, dass eine Spannungsversorgung des Terminals (2) überwacht wird und im Falle einer erkannten Änderung der Spannungsversorgung der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder gespeicherte Schlüssel gelöscht werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, *dadurch gekennzeichnet*, dass der Benutzer des Terminals (2) identifiziert wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, *dadurch gekennzeichnet*, dass die über das Netzwerk (1) gesendeten Daten verschlüsselt und die über das Netzwerk (1) empfangenen

Daten entschlüsselt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, *dadurch gekennzeichnet*, dass die Echtzeit überwacht wird und im Fehlerfall der Zugriff auf die gespeicherten Schlüssel gesperrt wird oder die gespeicherten Schlüssel gelöscht werden.

Hiezu 3 Blatt Zeichnungen

österreichisches
patentamt

AT 505 459 B1 2009-07-15

Blatt: 1

Int. Cl.[8]: G06F 21/06
H04L 9/10
G06F 12/14

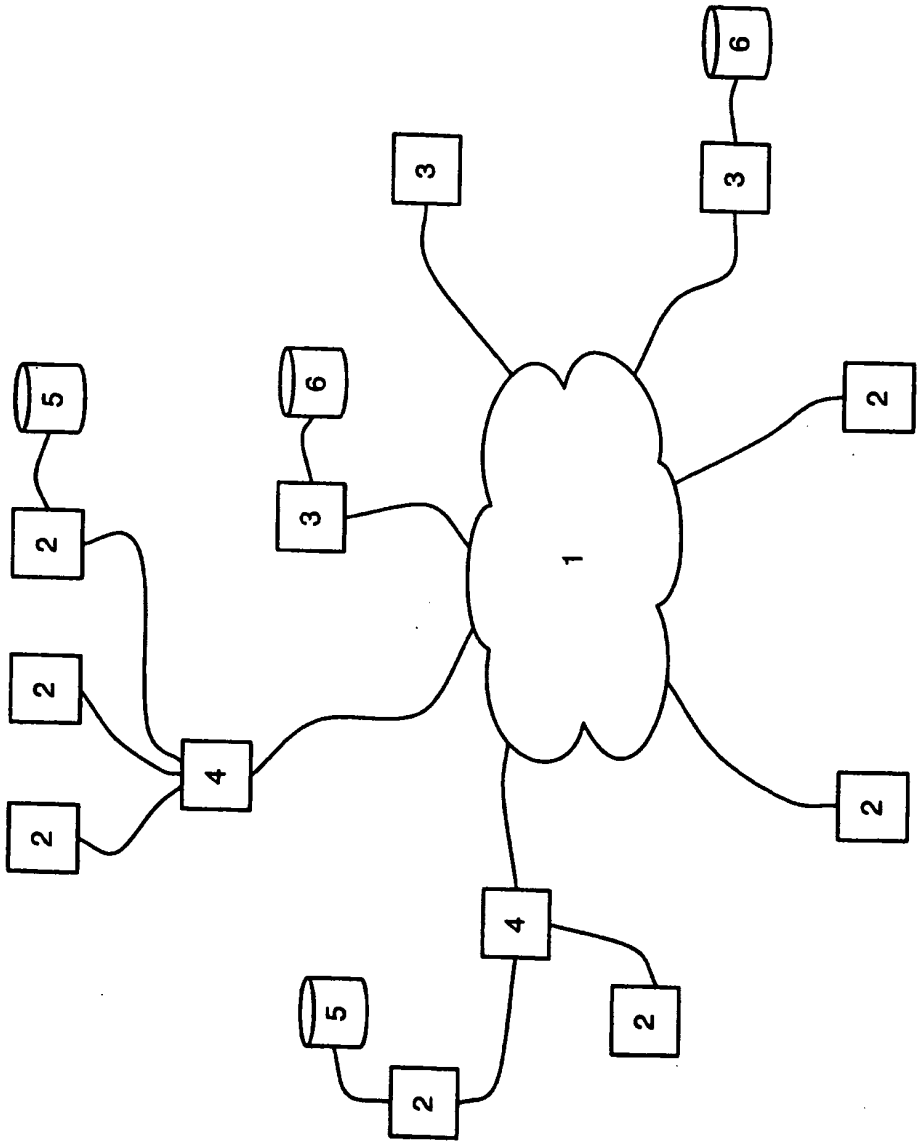

Fig. 1

Int. Cl.[8]: G06F 21/06
H04L 9/10
G06F 12/14

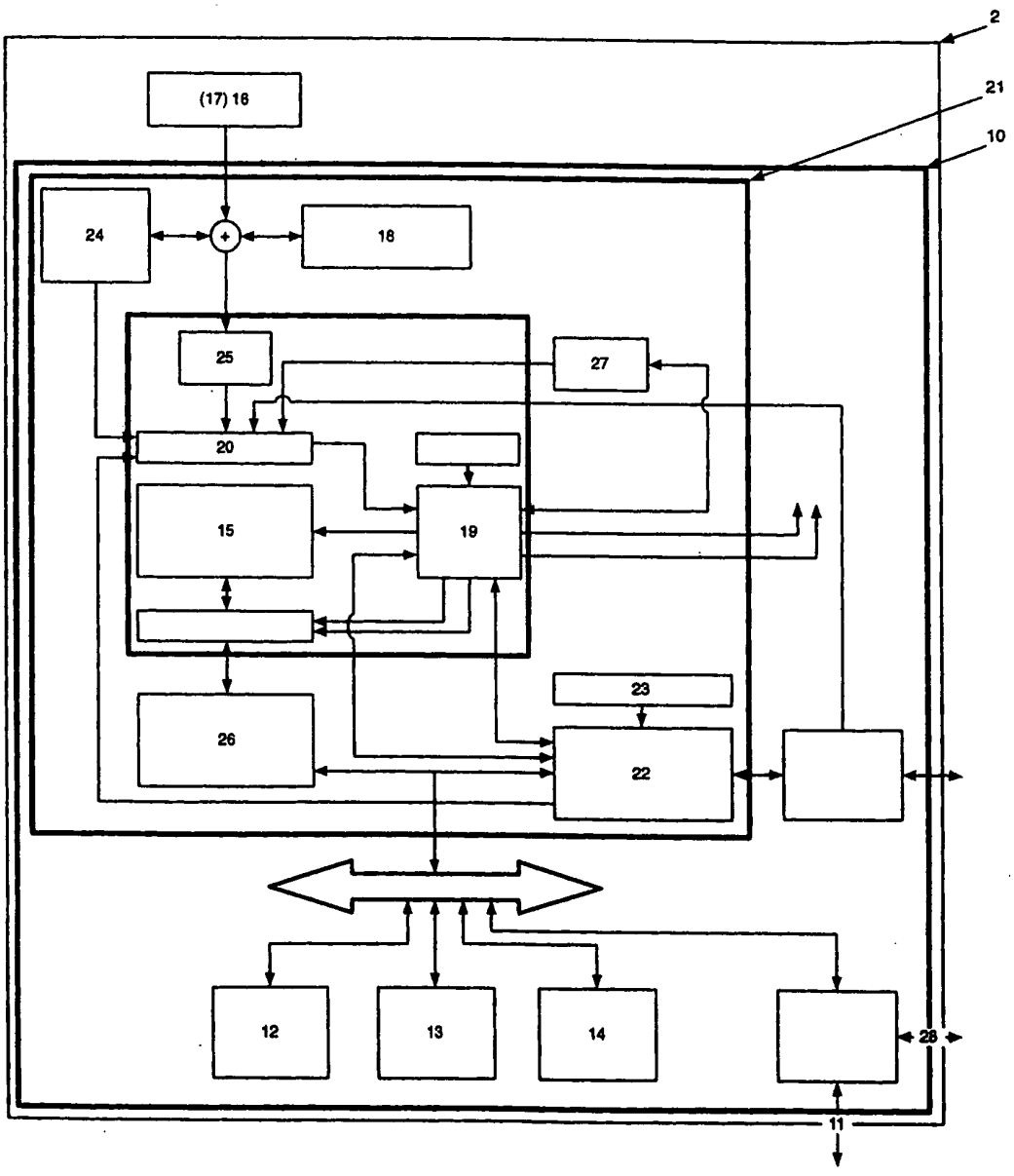

Fig. 2

Int. Cl.[8]: G06F 21/06
H04L 9/10
G06F 12/14

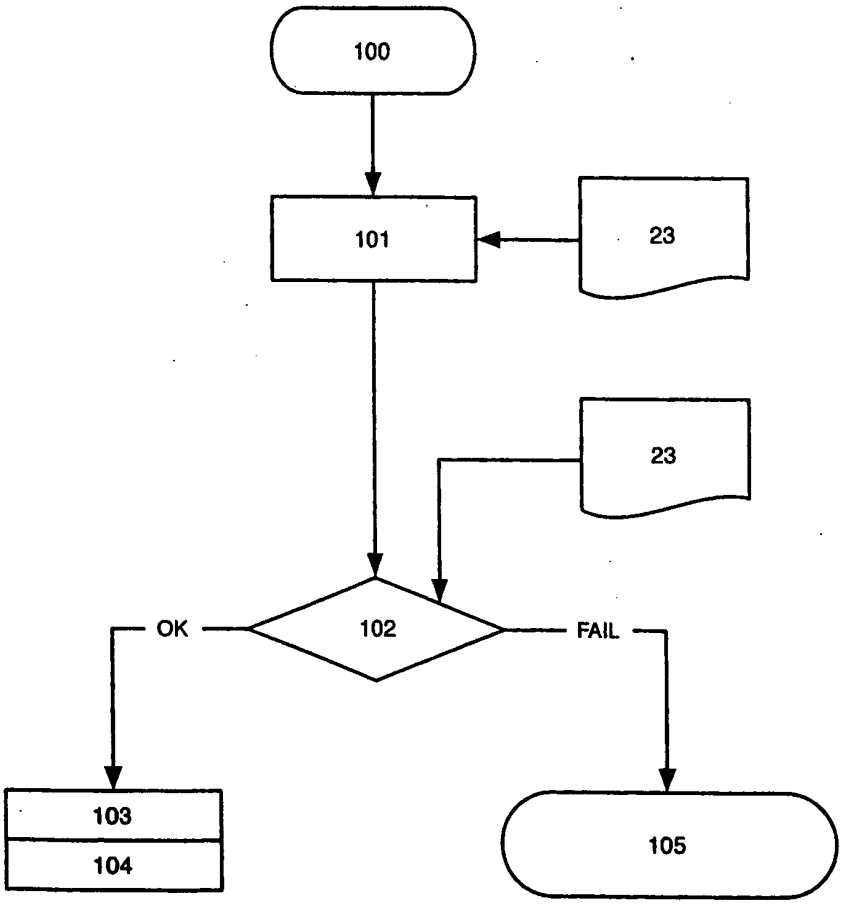

Fig. 3