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

(10) **DE 600 15 757 T2** 2005.12.08

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 190 289 B1**
(21) Deutsches Aktenzeichen: **600 15 757.1**
(86) PCT-Aktenzeichen: **PCT/FI00/00448**
(96) Europäisches Aktenzeichen: **00 927 294.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/70427**
(86) PCT-Anmeldetag: **18.05.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **23.11.2000**
(97) Erstveröffentlichung durch das EPA: **27.03.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **10.11.2004**
(47) Veröffentlichungstag im Patentblatt: **08.12.2005**

(51) Int Cl.[7]: **G06F 1/00**
G06F 12/14

(30) Unionspriorität:
991134 **18.05.1999** **FI**

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

(73) Patentinhaber:
SmartTrust Systems Oy, Sonera, FI

(74) Vertreter:
PAe Reinhard, Skuhra, Weise & Partner GbR, 80801 München

(72) Erfinder:
HILTUNEN, Matti, FIN-02150 Espoo, FI;
MIETTINEN, Jarmo, FIN-02600 Espoo, FI;
NORDBERG, Marko, FIN-00180 Helsinki, FI;
LIUKKONEN, Jukka, FIN-00530 Helsinki, FI

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG UM EIN PROGRAMMCODE ZU BEGLAUBIGEN**

Beschreibung

TECHNISCHER BEREICH

[0001] Die Erfindung betrifft Kommunikationssysteme. Eine bestimmte Aufgabe der Erfindung ist ein Verfahren und eine Vorrichtung zum Testen der Verlässlichkeit einer Software.

[0002] Die Aufgabe der Erfindung ist ein Verfahren zur Authentifizierung eines Programms oder eines Programmcodes bereitzustellen, welcher in einer Speichervorrichtung gespeichert ist, wobei durch diese Methode eine erste Prüfsumme in dem Programmcode berechnet wird, die Prüfsumme mit einer zweiten als gültig bekannten Prüfsumme verglichen wird und ansprechend auf den zuvor genannten Vergleich als gültig anerkannt wird, wenn die erste Prüfsumme mit der zweiten Prüfsumme übereinstimmt.

HINTERGRUND DER ERFINDUNG

[0003] Mobile Netzwerke, z.B. GSM-Netzwerke (GSM, Globales System für mobile Kommunikation) sind letztens sehr bekannt geworden. Entsprechend werden die mit den mobilen Netzwerken verbundenen zusätzlichen Dienste in hoher Geschwindigkeit erweitert. Die Verwendungsbereiche sind sehr vielfältig. Die Mobiltelefone können als Zahlungsmittel verwendet werden, z.B. für geringfügige Einkäufe, wie Softdrinks und die Benutzung von Autowaschanlagen. Tägliche Aktivitäten, wie z.B. Zahlungsüberweisungen, Bankdienste etc. wurden hinzugefügt und werden ebenso in der Zukunft zu der Funktionalität der herkömmlichen Mobiltelefone hinzugefügt. Die mobilen Stationen der nächsten Generation werden bezogen auf das Dienstleistungsniveau und die Datentransferkapazität fortschrittlicher verglichen mit vorhergehenden Generationen.

[0004] Mit Hilfe einer digitalen Signatur, welche als eine allgemeine Notwendigkeit für eine elektronische Zahlung angesehen wird, ist es möglich, die Kohärenz der zu sendenden Informationen sicherzustellen und die Quellenadresse zu identifizieren. Die digitale Signatur wird durch Verschlüsseln der Prüfsumme erhalten, welche mit einem privaten Schlüssel eines Absenders aus der zu sendenden Information berechnet wird. Da niemand außer dem Sender den privaten Schlüssel kennt, kann der Empfänger durch Dekodieren der Verschlüsselung mit dem öffentlichen Schlüssel des Absenders sicherstellen, dass die Information unverändert ist und unter Verwendung des privaten Schlüssels erzeugt wurde, welcher nur dem Absender bekannt ist. Ein Beispiel für einen in der digitalen Verschlüsselung verwendeten Algorithmus ist ein RSA-Chiffrierungs-Algorithmus, welcher ein Verschlüsselungssystem mit einem öffentlichen Schlüssel und einem privaten Schlüssel ist und welcher ebenso für verschlüsselte Botschaften verwendet wird.

[0005] In der Infrastruktur des öffentlichen Schlüssels behält der Benutzer nur den privaten Schlüssel bei sich, wohingegen der öffentliche Schlüssel für alle Teilnehmer verfügbar ist. Es reicht nicht, dass der öffentliche Schlüssel als solcher gespeichert wird, z.B. in einem elektronischen Mailverzeichnis, da jemand ihn fälschen könnte und als authentischer Besitzer des Schlüssels erscheinen könnte. Anstatt dessen werden eine Zertifizierung und Zertifikate benötigt, welche durch die vertrauenswürdige Partei (Zertifizierungsbehörde) ausgegeben werden und als Nachweis für die Tatsache dienen, dass der Name, Identifizierungsnummer und öffentlicher Schlüssel zu der gleichen Person gehören. Das Zertifikat ist gewöhnlicherweise eine Kombination, bestehend aus einem öffentlichen Schlüssel, einem Namen und einer Identifizierungsnummer etc., welche die Zertifizierungsbehörde mit ihrem privaten Schlüssel signiert.

[0006] Wenn der Empfänger einer digital unterzeichnenden Botschaft die Authentizität der Botschaft sicherstellen möchte, muss er/sie zuerst das digitale Zertifikat erhalten, welche ihm/ihr den öffentlichen Schlüssel und den Namen gibt. Danach hat er/sie das Zertifikat zu authentifizieren. Um in der Lage zu sein, dies auszuführen, kann er/sie mehrere weitere Zertifikate benötigen (Zertifizierungskette), welche verwendet werden, um das fragliche Zertifikat zu authentifizieren.

[0007] Im Fall, dass das Zertifikat authentisch ist, authentifiziert der Empfänger die Botschaft unter Verwendung des öffentlichen Schlüssels, welcher mit dem Zertifikat empfangen wurde. Falls die Signatur den Test besteht, ist der Absender die Person, welche durch das Zertifikat identifiziert wird. In der Zertifizierung wird eine spezielle Blockliste verwendet, in welcher die abgelaufenen Zertifikate außer Verwendung eingetragen werden. Verzeichnisdienste werden für die Zertifikate und die Blockliste benötigt.

[0008] Mobile Telefone wurden unter Verwendung von mindestens teilweise integrierten Systemen und Software implementiert. In diesem Fall ist eine Modifikation der Originalsofware und von Funktionen zumindest teilweise möglich. Mit einer modifizierten Software kann der Inhalt von elektronischen Zahlungsbotschaften mit betrügerischen Absichten geändert werden, durch Ändern der Kontonummern, zu zahlender Beträge, digitaler Signaturen etc. und zur gleichen Zeit der Benutzer mit den korrekten Informationen über die Transaktionen versorgt werden.

[0009] Heute ist es für einen Benutzer unmöglich zu prüfen, ob das von ihm benutzte Mobiltelefon mit der Originalsoftware von dem Hersteller oder mit einer geänderten Version versehen ist. Im Fall, dass das Mobiltelefon für Bankdienste verwendet wird, als ein

Zahlungsmittel etc., muss der Benutzer in der Lage sein zu überprüfen, ob die Vorrichtung mit der gültigen Originalsoftwareversion versehen ist.

[0010] Der wichtigste Punkt für den Benutzer ist in der Lage zu sein, die Verlässlichkeit der Anzeige und der Tastatur, die Sicherheit, die Echtheit der Teile, welche mit der Sicherheit verbunden sind, so wie die Abonnentenidentifikationsdaten, die Passwörter und Schlüsselcodes, wie auch die Sicherheit und Verlässlichkeit der Kommunikationskanäle, welche von der Vorrichtung verwendet werden, zu überprüfen. Zusätzlich muss der Benutzer in der Lage sein, die Software zufällig zu testen, zu einem unvorhergesehenen Zeitpunkt, so dass die Software nicht zuvor auf eine Prüfung eingerichtet ist.

[0011] Im Prinzip kann eine Software unter Verwendung einer sogenannten direkten Prüfung geprüft werden, in welcher zwei unabhängige genug effektive Prüfsummen auf der Mobiltelefon-Software berechnet werden, z.B. unter Verwendung einer Hash-Funktion SHA-1, MD5 oder einer equivalenten und effektiven Hash-Funktion. Die erste Prüfsumme wird auf dem Mobiltelefon berechnet und die zweite Prüfsumme wird durch einen Anbieter der Originalsoftware berechnet. Die erste und die zweite Prüfsumme werden miteinander verglichen und in dem Fall, dass sie übereinstimmen, ist die Software auf dem Telefon die Orginalsoftware. Das Problem mit dieser genannten Lösung ist jedoch die Tatsache, dass eine veränderte oder gefälschte Software die programmatische Berechnung, welche in dem Programm codiert ist, ignorieren kann und nur die Originalprüfsumme ausgibt, als wäre sie die erste Prüfsumme, wenn sie der Benutzer abfrägt.

[0012] WO-A2-9 810 611 und US-A-5 224 160 offenbaren die Merkmale, welche in der Präambel der unabhängigen Ansprüche festgelegt sind.

AUFGABE DER ERFINDUNG

[0013] Die Aufgabe der Erfindung ist die zuvor genannten Nachteile zu beseitigen oder zumindest zu reduzieren. Eine besondere Aufgabe der vorliegenden Erfindung ist ein Verfahren und eine Vorrichtung für eine verlässliche Prüfung der Authentizität und Gültigkeit von Software in einer mobilen Station zu offenbaren, obwohl die Erfindung zum Testen von jeder Art von Software verwendet werden kann.

[0014] Eine weitere Aufgabe der Erfindung ist ein verlässliches und änderbares Verfahren zu offenbaren durch welches verschiedene Dienstleistungsanbieter und Benutzer der Dienste die Authentizität der von ihnen benutzten Vorrichtungen und Programmen sicherstellen können.

[0015] Auf die kennzeichnenden Merkmale der Erfindung wird in den Ansprüchen Bezug genommen.

ZUSAMMENFASSUNG DER ERFINDUNG

[0016] Das Grundprinzip des erfindungsgemäßen Verfahrens wird in den Ansprüchen beansprucht.

[0017] In einer Anwendung der Erfindung kann ein authentifizierter Programmcode für die Authentifizierung von anderen Programmcodes verwendet werden, welche in der gleichen Software oder dem System beinhaltet sind, in solch einer Weise, dass die Prüfsumme des authentifizierten Programmcodes mit der einen verglichen wird, welche durch andere Programmcodes über die selbe Anfrage bereitgestellt wird. Dies betrifft z.B. die Verwendung eines authentifizierten Programmcodes eines ersten Benutzers für die Authentifizierung des Programmcodes eines zweiten Benutzers. In einer anderen Anwendung kann das Mobiltelefon des ersten Benutzers eine Botschaft zu dem Mobiltelefon des zweiten Benutzers senden. Die Botschaft würde die Anforderung informieren, welche der Benutzer der zweiten Mobilstation zum Testen seiner/ihrer Software verwenden könnte. Die gleiche Lösung kann zum automatischen Testen verwendet werden, in der Weise, dass ein Netzwerk, z.B. während der Initialisierung eines Anrufs, eine Anforderung an das Telefon sendet, auf welche das Telefon durch Senden der berechneten Prüfsumme antwortet. Falls die Prüfsumme nicht gültig ist, trifft das Netzwerk die notwendigen Schlussfolgerungen und informiert den Benutzer wie auch andere notwendige Parteien über die Angelegenheit.

[0018] Ein Vorteil der Erfindung verglichen mit dem Stand der Technik ist die Tatsache, dass aufgrund der Erfindung integrierte Systeme oder Software, welche als verlässlich bekannt sind, implementiert werden können, wobei deren Verlässlichkeit nach gewissen Zeitspannen geprüft werden kann.

[0019] Ein weiterer Vorteil der Erfindung im Vergleich mit dem Stand der Technik ist die Tatsache, dass das Berechnen der Prüfsumme keine externen Funktionen benötigt, sondern in die zu prüfende Software integriert werden kann. Darüber hinaus wird das Verfahren des öffentlichen Schlüssels und des privaten Schlüssels unnötig.

[0020] Zusätzlich wird weniger RAM benötigt, da der Programmcode nicht in der Vorrichtung dekodiert oder modifiziert werden muss. Zudem ist aufgrund der Dynamik der Anforderungen und der darauf antwortenden Prüfsumme kann die Prüfsumme zugehörig zu der Anforderung nicht vorher bekannt sein. In diesem Fall kann die Erstellung der Anforderungen vollständig zufällig erfolgen.

ZEICHNUNGEN

[0021] In dem folgenden Abschnitt wird die Erfindung mit Bezug auf die beigefügten Zeichnungen beschrieben, in welchen:

[0022] Fig. 1 schematisch eine Vorrichtung der Erfindung darstellt;

[0023] Fig. 2 die Funktion wie in der Erfindung beschrieben unter Verwendung eines Blockdiagramms darstellt; und

[0024] Fig. 3 ein Beispiel einer Berechnung der Prüfsumme wie in der Erfindung beschrieben darstellt.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0025] Die Vorrichtung in Fig. 1 weist einen Speicher **1**, einen Prozessor **2**, einen Empfangsbereich **3**, eine Anzeige **4** und eine Eingabevorrichtung **5** auf. Der Speicher ist in einen statischen Teil A und einen dynamischen Teil B unterteilt. Die Größe des dynamischen Teils B ist so gewählt, dass die der Anforderung der Prüfsumme zugeordnet ist, nicht passend ist, um darin gespeichert zu werden, um eine Täuschung möglichst zu verringern. Der Speicher **1**, der Empfangsbereich **3**, die Anzeige **4** und die Eingabevorrichtung **5** sind mit einem Prozessor **2** verbunden. Ein Beispiel einer Vorrichtung, wie in Fig. 1 dargestellt, kann eine Mobilstation sein, welche eine zentrale Berechnungseinrichtung zusammen mit den Prozessoren **2** und den Speichern **1**, dem Empfangsbereich **3**, der Anzeige **4** und der Tastatur aufweist. Wesentlich bezüglich der besagten Erfindung ist nicht die Vorrichtung selbst, durch deren Verwendung die Erfindung realisiert wird, sondern vielfältige Vorrichtungen sind möglich, welche in elektronischen Übertragungen verwendet werden.

[0026] Zusätzlich weist die Vorrichtung, wie in Fig. 1 dargestellt, eine Einrichtung **12** zum Berechnen der Prüfsumme des Programmcodes auf, eine Einrichtung **6** zum Addieren der vorbestimmten Anforderung des Programmcodes und eine Einrichtung **7** zum Berechnen der zuvor genannten ersten Prüfsumme aus der Kombination des Programmcodes und der Anforderung. In einer Anwendung können die Einrichtungen **7** und **12**, z. B. unter Verwendung eines zertifizierten Programmcodes implementiert werden, wobei sie in diesem Fall in dem Speicher gespeichert werden.

[0027] Zudem weist die Vorrichtung, wie in Fig. 1 dargestellt, eine Einrichtung **8** zum Speichern des Programms und der Anforderung in dem Speicherbereich und eine Einrichtung **9** zum Berechnen der Prüfsumme des gesamten statischen Speicherbereichs auf, wobei der zuvor genannte Programmcode und die Anforderung gespeichert werden. Außerdem weist die Vorrichtung eine Einrichtung **10** zum Empfangen der Anforderung der Speichervorrichtung über eine Tastatur **5** auf.

[0028] Fig. 2 stellt die Funktion der Erfindung in einem Blockdiagramm dar. Der Generator **26** der Anforderung und der Prüfsumme ist eine außenstehende Zertifizierungsbehörde, jemand anderes als der Benutzer **27**, z.B. der Hersteller des Programms oder eine vertrauenswürdige dritte Partei, welche den Original-Programmcode besitzt. Der Benutzer empfängt die Botschaft und die entsprechenden Prüfsumme, Pfeil **20**, von der außenstehenden Zertifizierungsbehörde, z.B. von einer sicheren Internetseite. Der Benutzer **27** aktiviert den Prüfbefehl der Vorrichtung, Pfeil **21**. Die Vorrichtung frägt den Benutzer nach der Anforderung, welche er/sie in die Vorrichtung eingibt, Pfeil **22**. Die Vorrichtung ist z.B. ein Mobiltelefon. Der Programmcode wird gemäß dem Algorithmus **28** gelesen, Pfeile **23** und **24**, und die Prüfsumme wird unter Verwendung eines geeigneten Verfahrens berechnet. Der Programmcode ist in dem Programmspeicher **29** angeordnet. Die Prüfsumme kann z.B. unter Verwendung einer Hash-Funktion berechnet werden. Hash-Funktionen sind z.B. MD5 und SAH-1. Die Prüfsumme, welche sich aus der Anwendung des Algorithmus **28** ergibt, wird dem Benutzer **27** zurückgegeben, welcher sie anforderte, Pfeil **25**. Der Benutzer **27** liest die berechnete Prüfsumme. z.B. auf der Anzeige von seinem ihrem Mobiltelefon und vergleicht sie mit der Prüfsumme, welche von der außenstehenden Zertifizierungsbehörde übergeben wird. Falls die Prüfsummen übereinstimmen, ist der Programmcode gültig.

[0029] Wesentlich in dem Verfahren zum Realisieren der Überprüfung ist die Tatsache, dass die Anforderung nicht zuvor bekannt ist. Aufgrund dessen ist die Prüfsumme zu der zugehörigen Anforderung unmöglich vorherzusehen. Die Anforderung, welche eingegeben wird, muss zusätzlich dazu lang genug sein, um die gewünschte Verlässlichkeit zu gewinnen. Weiter ist die Prüfsumme selbst nicht eine Eingabe in das Programm, wobei in diesem Fall das Programm sich selbst nicht auf die Umstände in Übereinstimmung mit der Prüfsumme anpassen kann. Während der Erzeugung der Prüfsumme wird der gesamte zu prüfende Programmcode unter Verwendung eines Algorithmus gelesen. Die Anforderung und der Programmcode werden so kombiniert, dass das Programm nicht die Kombination des Ergebnisses der Überprüfung und der Anforderung zugehörig zu dem Original-Programmcode berechnen kann und somit konsequenterweise zu der richtigen Schlussfolgerung kommt.

[0030] Fig. 3 stellt ein bevorzugtes Beispiel einer Erstellung der Prüfsumme gemäß der Erfindung dar.

Der Benutzer wünscht die Originalität der Software zu überprüfen, welche er/sie verwendet, wie in der Erfindung beschrieben. Zur Überprüfung wurde eine zufällige Anforderung **30** erstellt, unter Verwendung welcher die Überprüfung ausgeführt wird. In diesem Beispiel ist die Überprüfung **30** eine Buchstaben-Zeichenfolge, welche aus den Buchstaben A, B, W, U, M und E besteht. Jeder der Buchstaben der Anforderung **30** ist irgendwo in dem Speicherbereich **31** angeordnet. Der Anordnungsbereich ist durch den Anordnungsalgorithmus **32** festgelegt. Der Anordnungs-Algorithmus arbeitet, z.B. in einer Weise, dass das Zeichen, welches in der Anforderung beinhaltet ist, zu einer gewissen Speicheradresse des Speicherbereichs **31** addiert wird oder alternativ in der Weise, dass eine gewisse Berechnungsoperation zwischen den Buchstaben und dem Inhalt einer gewissen Speicheradresse ausgeführt wird, wobei das Ergebnis in der besagten Speicheradresse angeordnet ist. Pfeil **33** zeigt das Verfahren des Prüfalgorithmus. Wenn alle Zeichen, welche in der Anforderung beinhaltet sind, in dem Speicherbereich **31** wie gewünscht lokalisiert wurden, wird eine Prüfsumme über den gesamten Speicherbereich unter Verwendung z.B. eines Hash-Algorithmus berechnet. Als ein Beispiel für einen Hash-Algorithmus seien der MD5 und der SAH-1 Algorithmus genannt.

Patentansprüche

1. Verfahren zum Authentifizieren eines Programmcodes, welcher in einer Speichervorrichtung gespeichert ist, wobei das Verfahren die Schritte aufweist:
– Berechnen einer ersten Hashfunktion aus dem Programmcode;
– Vergleichen eines Hashwertes mit einem zweiten Hashwert, welcher als gültig bekannt ist; und
– der Programmcode wird als gültig anerkannt als Reaktion auf den zuvor genannten Vergleich, falls der erste Hashwert mit dem zweiten Hashwert übereinstimmt;
dadurch gekennzeichnet,
dass das Verfahren die Schritte aufweist:
– Speichern und Eingeben einer Anforderung in die Speichervorrichtung zu einem zufälligen Zeitpunkt zum Prüfen der Authentifizierung der Software, welche in der Speichervorrichtung gespeichert ist;
– Addieren der Anforderung zu dem Programmcode, wobei die Anforderung aus einer Gruppe gewählt wird, welche eine Zeichenfolge, eine Programmfunktion und eine Eingabe zum Bilden einer Kombination mit dem Programmcode und der Anforderung beinhaltet; und
– Berechnen der zuvor genannten ersten Hashfunktion aus der zuvor genannten Kombination.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine neue Anforderung oder ein Satz neuer Anforderungen und zugehöriger Hashwert (e) durch den Hersteller der Originalsoftware bekannt gegeben werden.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass eine neue Anforderung oder ein Satz neuer Anforderungen regelmäßig bekannt gegeben werden.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anforderung und/oder der Hashwert aus einer Datenbank oder von einem Medientyp abgefragt werden, welche zum Erhalten der Anforderungen und/oder des Hashwertes zugänglich sind.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anforderung und der zu der Anforderung zugehörige Hashwert aus einer zufälligen Gruppe ausgewählt werden, welche aus einem Satz an Anforderungen und zu den Anforderungen zugehörigen Hashwerten besteht.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anforderung einem externen Endgerät, einer externen Zertifizierungsbehörde oder einem Kommunikationsnetzwerk in einer Initialisierungsphase übermittelt wird.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass ein bestimmter Teil des Programmcodes durch die Anforderung ersetzt wird, bevor die Hashfunktion berechnet wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Verfahren die Schritte aufweist:
– Speichern des Programmcodes und der Anforderung in einem Speicherplatz; und
– Berechnen der ersten Hashfunktion auf dem gesamten Speicherplatz, in welchem der zuvor genannte Programmcode und die Anforderung gespeichert sind.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Länge der Anforderung derart gewählt wird, dass freigegebener Speicher nicht zum Speichern der den Anforderungen zugehörigen Hashwerte benutzt werden kann.

10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass ein authentifizierter Programmcode zum Authentifizieren eines anderen Programmcodes, welcher in derselben Software oder System enthalten ist, verwendet wird, so dass der Hashwert des authentifizierten Programmcodes mit dem Hashwert verglichen wird, welcher durch andere Programmcodes über dieselbe Anforderung gegeben ist.

11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Verfahren zusätzlich eine Verbindung der Speichervorrichtung mit der Außenwelt ver-

hindert; und
die Gültigkeit des Programmcodes in der Speichereinrichtung verifiziert wird.

12. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anforderung, welche zu dem Programmcode addiert wird, durch Verwenden bestimmter Algorithmen verändert wird, um eine Anforderung eines Standardformats zu erhalten.

13. Vorrichtung zum Authentifizieren des Programmcodes, wobei die Vorrichtung folgende Einrichtungen aufweist:
– eine Datenverarbeitungseinrichtung (**1**);
– eine Speichervorrichtung (**2**), welche mit der zuvor genannten Datenverarbeitungseinrichtung (**1**) verbunden ist;
– eine Einrichtung (**12**) zum Berechnen einer Hashfunktion auf dem Programmcode;
– eine Anzeigeeinrichtung (**4**), welche mit der zuvor genannten Datenverarbeitungseinrichtung verbunden ist; und
– eine Tastatur (**5**), welche mit der zuvor genannten Datenverarbeitungseinrichtung (**1**) verbunden ist;
dadurch gekennzeichnet, dass die Einrichtung aufweist:
– Mittel (**6**) zum Addieren einer vorbestimmten Anforderung zu dem Programmcode, welche aus einer Gruppe bestehend aus einer Zeichenfolge, einer Programmfunktion und einer Eingabe gewählt wird, wie auch Mittel zum Bilden einer Kombination des Programmcodes und der Anforderung; und
– Mittel (**7**) zum Berechnen der ersten Hashfunktion der zuvor genannten Kombination.

14. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass die Vorrichtung aufweist:
– Mittel (**8**) zum Speichern des Programmcodes und der Anforderung in einem statischen Speicherplatz; und
– Mittel (**9**) zum Berechnen der Hashfunktion auf dem gesamtem statischen Speicherplatz, in welchem der Programmcode und die Anforderung gespeichert sind.

15. Vorrichtung nach einem der Ansprüche 13 oder 14, dadurch gekennzeichnet, dass die Vorrichtung Mittel (**3**) zum Empfangen der Anforderung in der Speichervorrichtung mittels einer Tastatur (**5**) aufweist.

16. Vorrichtung nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass die Vorrichtung Mittel (**10**) zum Abfragen der Anforderung und/oder eines Hashwertes von einer Datenbank oder einem Medientyp aufweist, auf welchen zugegriffen werden kann, um die Anforderung und/oder den Hashwert zu erhalten.

17. Vorrichtung nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, dass die Vorrichtung Mittel (**11**) zum Empfangen der Anforderung von einem externen Endgerät, einer externen Zertifizierungsbehörde oder einem Kommunikationsnetzwerk in einer Initialisierungsphase aufweist.

18. Vorrichtung nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass die Vorrichtung Mittel (**13**) zum Ersetzen eines bestimmten Teils des Programmcodes vor dem Berechnen der Hashfunktion aufweist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

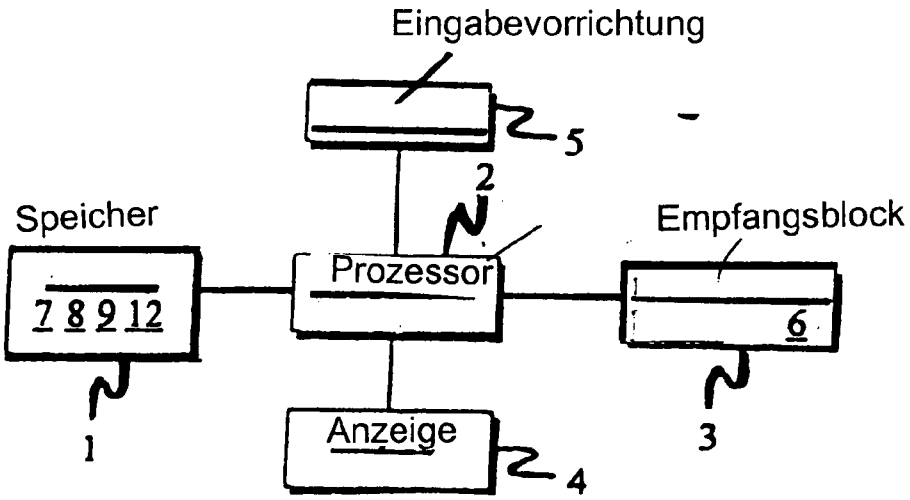

Fig. 1

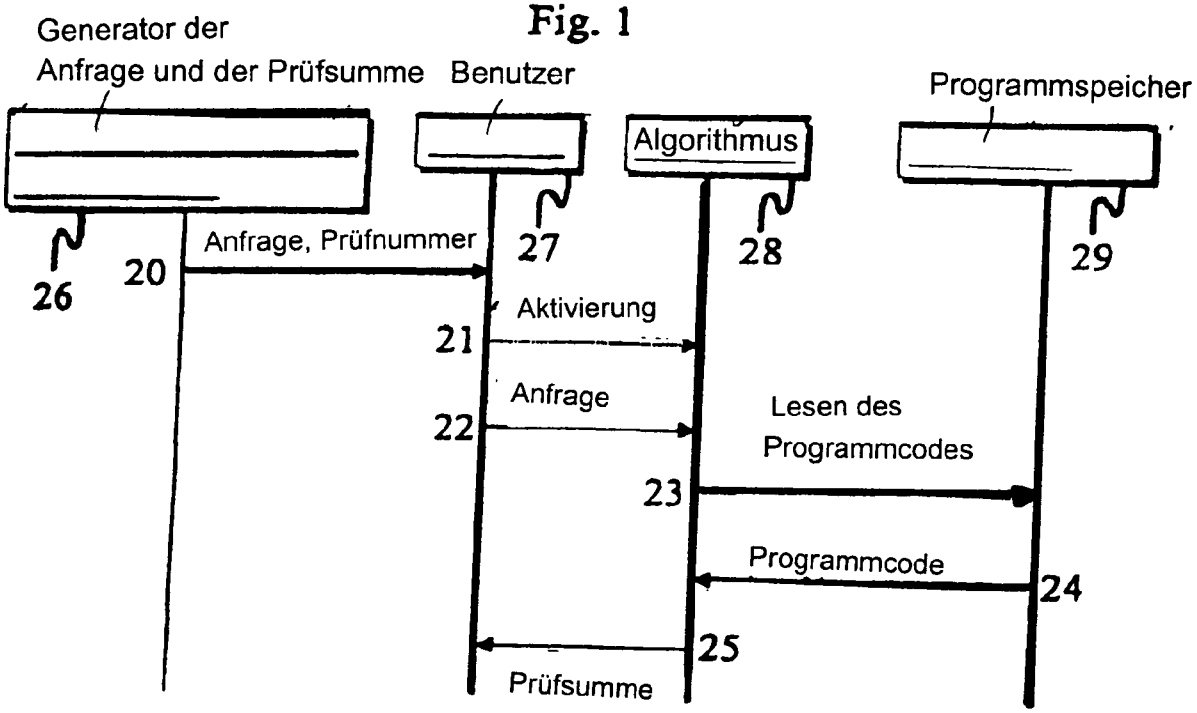

Fig. 2

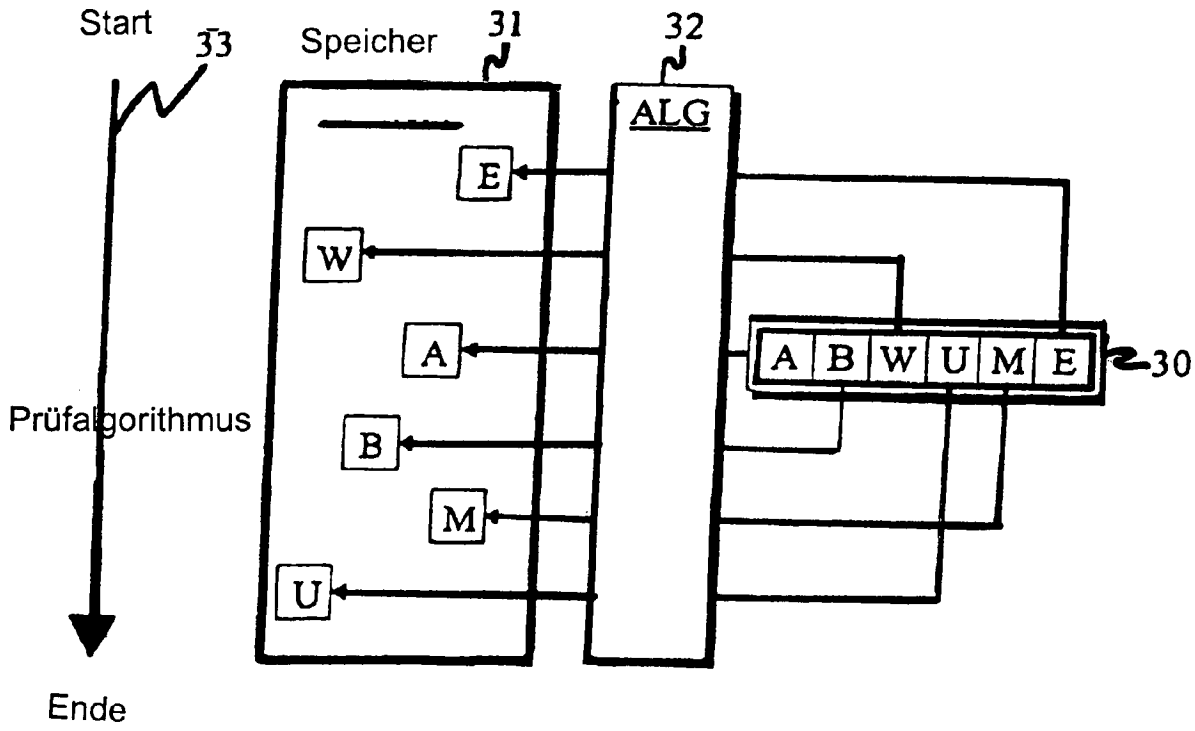
Start
33
Speicher
31
32
ALG
E
W
A
B
M
U
A B W U M E
30
Prüfalgorithmus
Ende

Fig. 3