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

(10) **DE 696 28 321 T2** 2004.04.29

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 861 541 B1**
(21) Deutsches Aktenzeichen: **696 28 321.2**
(86) PCT-Aktenzeichen: **PCT/US96/18037**
(96) Europäisches Aktenzeichen: **96 941 986.0**
(87) PCT-Veröffentlichungs-Nr.: **WO 97/018655**
(86) PCT-Anmeldetag: **14.11.1996**
(87) Veröffentlichungstag der PCT-Anmeldung: **22.05.1997**
(97) Erstveröffentlichung durch das EPA: **02.09.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.05.2003**
(47) Veröffentlichungstag im Patentblatt: **29.04.2004**

(51) Int Cl.[7]: **H04L 9/08**
H04L 9/30, H04L 9/32

(30) Unionspriorität:
555697 **14.11.1995** **US**

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

(73) Patentinhaber:
Microsoft Corp., Redmond, Wash., US

(74) Vertreter:
Dr. Pöhner und Kollegen, 97070 Würzburg

(72) Erfinder:
SPELMAN, F., Jeffrey, Duvall, US; THOMLINSON, W., Matthew, Bellvue, US

(54) Bezeichnung: **RÜCKGEWINNUNG EINES ANGEGRIFFENEN WURZEL-SCHLÜSSELS**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Die Erfindung bezieht sich allgemein auf Kryptographie und insbesondere auf die Wiederherstellung kompromittierter Wurzelschlüssel.

[0002] In Kryptographie wurden verschiedene Algorithmen entwickelt, auf die als öffentliche Schlüsselalgorithmen Bezug genommen wird. Sie sind für die Unterzeichnung und Authentifikation elektronischer Dokumente sehr nützlich.

[0003] Im allgemeinen involvieren öffentliche Schlüsselalgorithmen zwei Schlüssel, nämlich einen öffentlichen Schlüssel und einen privaten Schlüssel. Der private Schlüssel wird von der Zertifizierungsbehörde aufbewahrt und geheim gehalten; während der öffentliche Schlüssel, wie der Name schließen lässt, an die Öffentlichkeit verteilt wird. Der Inhaber des öffentlichen Schlüssels kann ihn dazu verwenden Daten zu verschlüsseln, die nur von einer Person entschlüsselt werden können, die über den privaten Schlüssel verfügt. Ebenso kann der Inhaber des privaten Schlüssels diesen auch dazu verwenden Daten zu verschlüsseln, die dann nur von der Person entschlüsselt werden können, die über den öffentlichen Schlüssel verfügt. Deshalb stellen beide Schlüssel ein nützliches Werkzeug für das Verschlüsseln von Dokumenten bereit, so dass sie nicht von Parteien gelesen werden können, für welche die Dokumentenicht beabsichtigt sind.

[0004] Bei Benutzen des privaten Schlüssels zum Verschlüsseln von Daten, wird das Ergebnis manchmal eine digitale Unterschrift genannt. Sie weist das besondere Merkmal auf, dass nur der Inhaber des privaten Schlüssels produziert haben könnte. Daher kann, wenn der private Schlüssel geheim gehalten wird, der Empfänger eines Dokuments mit einer digitalen Unterschrift die Quelle des Dokuments verifizieren, indem er die digitale Unterschrift verifiziert. Das Verifizieren der digitalen Unterschrift involviert einfach die Anwendung des öffentlichen Schlüssels auf die digitale Unterschrift, um eine Datenkette zu produzieren und diese dann mit dem Dokument zu vergleichen, dem die Unterschrift angehängt war. Ist die Datenkette dem angehängten Dokument identisch, dann kann der Empfänger zuversichtlich sein, dass das Dokument tatsächlich von der Zertifizierungsbehörde unterschrieben wurde und kann dem Inhalt des unterzeichneten Dokuments trauen.

[0005] Natürlich gilt das nur solange wie die Öffentlichkeit Vertrauen dazu hat, dass der private Schlüssel tatsächlich privat geblieben und nur der Zertifizierungsbehörde bekannt ist. Sobald der Schlüssel kompromittiert wird, kann der Empfänger eines unterzeichneten Dokuments nicht mehr sicher sein, dass das Dokument von der Zertifizierungsbehörde und nicht von einer Partei unterschrieben wurde, die den privaten Schlüssel kompromittiert hat. Wenn eine der Zertifizierungsbehörde übergeordnete Behörde vorhanden ist und der jeder traut (auf die wir als Zentralbehörde Bezug nehmen werden), dann kann die Zertifizierungsbehörde, deren Schlüssel kompromittiert wurde, einen neuen privaten Schlüssel selektieren und einen Ersatzschlüssel mit einer angehängten Zertifizierung der Zentralbehörde verteilen. Empfänger des Ersatzschlüssels werden, auf Grund der digitalen Unterschrift der Zentralbehörde, darauf vertrauen können, dass der neue öffentliche Schlüssel dem neuen privaten Schlüssel entspricht.

[0006] Was geschieht aber, wenn der private Schlüssel der Zentralbehörde kompromittiert wird? Und was geschieht, wenn es keine der Zentralbehörde übergeordnete. Behörde gibt, der jeder traut? Dann. wird das Problem, wie der Ersatzschlüssel wirksam und effizient zu verteilen ist, damit die Öffentlichkeit ihm als einem gültigen Schlüssel und nicht als einem Schlüssel vertrauen kann, der eigentlich einer Entität gehört, die versucht das System zu untergraben, zu einem sehr schwierig zu lösendem Problem.

[0007] In dieser Hinsicht, in D. Denning, "Schützen von öffentlichen Schlüsseln und privaten Schlüsseln", Computer, Februar 1983, Band 16, Nr. 2, Seiten 27–35, schlägt der Autor ein Verfahren für Feststellen kompromittierter Wurzelschlüssel vor, die auf der Verwendung von Unterschriftsprotokollen beruhen, die auf einem Schlüsselserver unterhalten werden, in dem jeder Protokolleintrag ein mit Uhrzeit und Datum gestempeltes Unterschriftszertifikat enthält, das einen privaten Schlüssel enthält. Dieses Verfahren verlässt sich auf extreme Schwierigkeit, auf die ein Dritteinbrecher, beim korrekten Einfügen eines gefälschten Zertifikats mit einer geeigneten Zeitfolge in das Protokoll, stoßen würde. Jedoch verabsäumt dieses Verfahren die Frage anzugehen wie der Empfänger den Ersatzschlüssel validieren kann, d. h. bestimmen kann ob jener Schlüssel und nicht der vom Einbrecher zur Verfügung gestellte gültig ist.

Zusammenfassung der Erfindung

[0008] Allgemein, in einer Hinsicht, ist die Erfindung ein Verfahren zum Ersetzen eines Wurzelschlüssels, der ein privater Schlüssel eines aus einem öffentlichen und einem privaten Schlüssel bestehenden Schlüsselpaars ist. Das Verfahren schließt die Schritte der elektronischen Sendung einer Meldung ein, die anzeigt, dass der Wurzelschlüssel ersetzt wird und einen Ersatzschlüssel und eine digitale Unterschrift enthält, die durch Verwendung des Wurzelschlüssels generiert wurde; und der Veröffentlichung in einem Außenbandkanal eines Werts V ein, wobei V aus der Meldung hergeleitet ist. Der Ersatzschlüssel ist der öffentliche Schlüssel eines weiteren aus einem öffentlichen und einem privaten Schlüssel bestehenden Schlüsselpaars, das das zuerst erwähnte, aus einem öffentlichen und einem privaten Schlüsel bestehende Schlüsselpaar ersetzt.

[0009] Bevorzugte Ausführungsbeispiele schließen folgende Merkmale ein. Das Verfahren schließt den Schritt der Berechnung des Werts V durch Anwen-

dung einer Einwegfunktion auf wenigstens einen Teil der Meldung ein. Außerdem schließt das Verfahren den Schritt der Verkettung des Ersatzschlüssels mit einer Kennung ein, um die Meldung zu generieren und die Kennung identifiziert die Meldung als eine Meldung, die einen Ersatzschlüssel trägt. Der die Meldung generierende Schritt schließt weiter die Verkettung des Ersatzschlüssels (1) mit einer Seriennummer, die anzeigt welcher einer Vielheit von Wurzelschlüsseln ersetzt wird; (2) mit einem "gut bis" Datum, das anzeigt wann der Ersatzschlüssel ablaufen wird; und (3) mit einem "gut ab" Datum, das eine Zeit anzeigt über die hinaus der Ersatzschlüssel aktiv werden wird, ein.

[0010] Allgemein, in einer weiteren Hinsicht, ist die Erfindung ein Verfahnen des Ersetzens eines Wurzelschlüssels, d. h. des privaten Schlüssels eines aus einem öffentlichen und einem privaten Schlüssel bestehenden Schlüsselpaars. Das Verfahren schließt die Schritte der, Generierung einer ersten Meldung, die einen Ersatzschlüssel und eine Anzeige einschließt, dass der Wurzelschlüssel ersetzt wird; Generierung einer digitalen Unterschrift durch Anwendung des Wurzelschlüssels auf die erste Meldung; Kombinieren der ersten Meldung und der digitalen Unterschrift zum Produzieren einer zweiten Meldung; elektronisches Senden einer zweiten Meldung; Veröffentlichung eines Werts V in einem Inbandkanal, der aus der zweiten Meldung hergeleitet wird, ein.

[0011] Allgemein, in noch einer weiteren Hinsicht, ist die Erfindung ein Reaktionsverfahren auf eine Änderung eines Wurzelschlüssels, d. h. des privaten Schlüssels eines aus einem öffentlichen und einem privaten Schlüssel bestehenden Schlüsselpaars. Aas Verfahren schließt die Schritte des elektronischen Empfangs einer Meldung, die anzeigt, dass der Wurzelschlüssel ersetzt wird und die außerdem einen Ersatzschlüssel und eine digitale Unterschrift enthält, die unter Verwendung des Wurzelschlüssels generiert wurde; Verwendung des dem öffentlichen Schlüssels entsprechenden Wurzelschlüssels zum Verifizieren der digitalen Unterschrift der Meldung; Erhalten, durch einen Außenbandkanal, eines von der Meldung hergeleiteten Werts, mittels Anwendung eines Algorithmus auf wenigstens einen Teil der Meldung; Anwendung des Algorithmus auf den besagten wenigstens einen Teil der Meldung, um einen Wert B zu generieren; Vergleichen von B mit V; und, falls B gleich V ist, Ersetzen des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht mit dem Ersatzschlüssel ein.

[0012] Allgemein, in einer noch weiteren Hansicht, ist die Erfindung ein Verfahren zur Wiederherstellung eines kompromittierten Wurzelschlüssels, einschließlich folgender Schritte: elektronischer Empfang einer Notmeldung, die anzeigt, dass der Wurzelschlüssel ersetzt wird und außerdem einen Ersatzschlüssel und eine digitale Unterschrift enthält, die mittels Verwendung des Wurzelschlussels generiert wurde; Verwendung des öffentlichen Schlüssels für den kompromittierten Wurzelschlüssel, um die digitale Unterschrift der Notmeldung zu verifizieren; Erhalten durch einen Außenkanal eines von der Notmeldung hergeleiteten Werts V, durch Anwendung eines Algorithmus auf wenigstens einen Teil der Notmeldung; Anwendung des Algorithmus auf die Notmeldung, um einen Wert B zu. generieren; Vergleichen von B mit V; und ob B gleich V ist, Ersetzen des kompromittierten öffentlichen Schlüssels mit dem Ersatzschlüssel.

[0013] Allgemein, in einer weiteren Hinsicht, ist die Erfindung eine Vorrichtung zur Wiederherstellung eines kompromittierten Wurzelschlüssels. Die Vorrichtung schließt einen digitalen Prozessor; eine an den Prozessor angeschlossene Kommunikationsschnittstelle und durch den eine Notmeldung elektronisch empfangen wird; Speicher, der den öffentlichen Schlüssel speichert, der dem Wurzelschlüssel entspricht; und eine Eingabeeinrichtung ein, durch die ein Wert V in den digitalen Prozessor eingegeben wird, wobei V durch einen Außenbandkanal erhalten wird und durch Anwenden eines Algorithmus auf wenigstens einen Teil der Notmeldung generiert wurde. Die Notmeldung zeigt an, dass der Wurzelschlüssel kompromittiert worden ist und enthält außerdem einen Ersatzschlüssel und eine digitale Unterschrift, die durch Verwendung des kompromittierten Wurzelschlüssels generiert wurde. Der digitale Prozessor ist programmiert den dem öffentlichen Schlüssel entsprechenden Wurzelschlüssel zu verwenden, um die digitale , Unterschrift der Notmeldung zu verifizieren; den Algorithmus auf die Notmeldung anzuwenden, um einen Wert B zu generieren; B mit V zu vergleichen; und den öffentlichen Schlüssel, der dem Wurzelschlüssel entspricht, mit dem Ersatzschlüssel zu ersetzen, wenn B gleich V ist.

[0014] Allgemein, in einer noch weiteren Hinsicht, ist die Erfindung ein maschinenlesbarer Datenträger, der ein Computerprogramm zur Wiederherstellung eines kompromittierten Wurzelschlüssel speichert. Das gespeicherte Programm schließt maschinenlesbare Instruktionen . ein:

[0015] (1) die bewirken, dass der Computer aus dem Speicher eine Notmeldung wiedergewinnt, die anzeigt, dass der Wurzelschlüssel kompromittiert worden ist und, die außerdem einen Ersatzschlüssel und eine digitale Unterschrift enthält, die durch Verwendung des kompromittierten Wurzelschlüssels generiert wurde; (2) die bewirken, dass der Computer den, dem Wurzelschlüssel entsprechenden, öffentlichen Schlüssel verwendet, um die digitale Unterschrift der Notmeldung zu verifizieren; (3) die bewirken, dass der besagte Computer den Algorithmus auf die Notmeldung anwendet, um einen Wert B zu generieren; (4) die bewirken, dass der Computer B mit V vergleicht; und (5) die bewirken, dass der Computer den, dem Wurzelschlüssel entsprechenden, öffentlichen Schlüssel mit dem Ersatzschlüssel ersetzt, falls B gleich V ist.

[0016] Wiederherstellung kompromittierter Wurzel-

schlüssel ist ein ernstes, ungelöstes Problem, das Kryptographie mit öffentlichen Schlüsseln plagt. Die Erfindung erlaubt einem Benutzer die Fähigkeit des Benutzer auszunutzen Schlüssel elektronisch, ohne die Gefahr des Versagens, aufgrund eines Ausschaltungsanschlags seitens des Kompromisslers des Schlüssels, zu empfangen, und ohne mühsames, manuelles Eintippen des ganzen Schlüssels in das System, das bis zu hunderten von Hex-Stellen involvieren könnte. Die Erfindung ermöglicht, durch Verwendung einer Einwegfunktion zum Generieren eines Verifizierungscode und durch anschließendes ausnutzen vorhandener Außenbandkanäle, die bereits verfügbar sind, eine sichere Wiedereingabe, indem der Benutzer nur 15–20 Hex-Stellen eingibt. Der viel größere Schlüssel kann elektronisch empfangen und eingegeben werden.

[0017] Durch Verwendung von Außenband-Authentifikationsverfahren, zusammen mit einer Notmeldung, kann der Benutzer viel Zuversicht bekommen, dass sowohl die Meldung als auch der Ersatzschlüssel-Authentifikationssschlüssel legitim sind.

[0018] Mit der Erfindung lässt sich eine Zwischenentität (beispielsweise ein Kaufmann) benachrichtigen, dass der Wurzelschlüssel kompromittiert worden ist. Danach kann, wenn der Kaufmann eine elektronische Kommunikation an einen Verbraucher sendet, jene Kommunikation außerdem. die Notmeldung einschließen, die den neuen öffentlichen Schlüssel für die Zentralbehörde enthält, sowie eine Benachrichtigung an den Verbraucher, dass dieses der neue zu verwendende öffentliche Schlüssel ist. Auf diese Weise kann sich die Zentralbehörde darauf verlassen, dass andere Entitäten helfen die Notmeldung zu verteilen und braucht nicht die Verantwortlichkeit zu tragen alle betroffenen Parteien benachrichtigen zu müssen.

[0019] Andere Vorteile und Merkmale werden anhand der folgende n Beschreibung der bevorzugten Ausführung und aus den Ansprüchen offenkundig werden.

Kurzbeschreibung der Zeichnungen

[0020] **Abb.** 1 zeigt das Format der Notmeldung;

[0021] **Abb.** 2 ist ein Flussdiagramm und zeigt die von einer Zentralbehörde bei der Wiederherstellung eines kompromittierten Wurzelschlüssels durchgeführten Maßnahmen;

[0022] **Abb.** 3 ist ein Flussdiagramm und zeigt die von einem Verbraucher bei der Wiederherstellung eines kompromittierten Wurzelschlüssels durchgeführten Maßnahmen; und

[0023] **Abb.** 4 ist ein Blockdiagramm eines Computersystems, das die Wiederherstellung des kompromittierten Wurzelschlüssels ausführt.

Beschreibung des bevorzugten Ausführungsbeispiels

Notmeldung

[0024] Allgemein involviert die Erfindung den Gebrauch eines Inbandkanals, um eine Notmeldung bezüglich eines kompromittierten Schlüssels zu verteilen, die einen neuen Ersatzschlüssel enthält und die Verwendung eines verschiedenen Außenbandkanals, um einen Verifizierungscode zu veröffentlichen, der von Kunden zur Verifizierung der Echtheit der Notmeldung benutzt werden kann. Mit einem Inbandkanal meinen wir jeden Kanal elektronischer Kommunikation, den die Parteien zur Durchführung ihrer normalen Geschäftstätigkeit miteinander verwenden. Diese können das Internet, Computerverbindungen wie beispielsweise weiträumige Netze (WAN), Telefonleitungen, Funkübertragungen oder jeweils eine oder mehrere, eine große Anzahl von Möglichkeiten, einschließen. Mit einem Außenbandkanal meinen wir irgendeinen anderen Kanal, der einer Entität ermöglicht mit der anderen Entität zu kommunizieren. Ein Außenbandkanal könnte nur unidirektionale Kommunikation ab der Zentralbehörde unterstützen; wie es beispielsweise für die Veröffentlichung in einer Zeitung der Fall wäre. Der Außenbandkanal sollte das Merkmal haben, dass der Empfänger der Außenband-Kommunikation hohe Zuversicht haben wird, dass die Meldung von der.

[0025] Zentralbehörde und nicht von irgendeiner Partei kam, die vorgibt die Zentralbehörde zu sein.

[0026] Mit Bezug auf **Abb.** I, eine Notmeldung 10 schließt eine Meldungskennung 12, eine Seriennummer 14, einen Ersatzschlüssel 16, ein "gut ab" Datum 18, ein "gut bis" Datum 20 und eine digitale Unterschrift ein. Die Meldungskennung 12 identifiziert die Meldung als eine Notmeldung. Die Seriennummer 14, die optional sein kann, identifiziert den speziellen Wurzelschlüssel, der kompromittiert worden ist. Dieses kann eine Notwendigkeit sein, insbesondere, wenn es mehr als ein, aus einem privaten Schlüssel und einem öffentlichen Schlüssel bestehendes, Schlüsselpaar gibt, das von der Zentralbehörde benutzt wird.

[0027] Der Ersatzschlüssel 16 ist der öffentliche Schlüsselteil des neuen aus einem privaten Schlüssel und einem öffentlichen Schlüssel bestehenden Schlüsselpaars, das selektiert worden ist den kompromittierten Wurzelschlüssel des vorhergehenden, aus einem privaten Schlüssel und einem öffentlichen Schlüssel bestehenden, Schlüsselpaars zu ersetzen.

[0028] Die zwei Datenfelder, die "gut ab" Daten 18 und "gut bis" Daten 20 enthalten, zeigen die Zeitspanne an, für die der Ersatzschlüssel gültig ist. Das "gut ab" Datum ist besonders indem Fall nützlich, wenn die Zentralbehörde eine Politik des periodischen Ersetzens seines, aus einem privaten Schlüssel und einem öffentlichen Schlüssel bestehenden, Schlüsselpaars als Teil eines Programms verfolgt die

fortdauernde Sicherheit ihres Systems sicherzustellen. In diesem Fall kann die Zentralbehörde die Notmeldung vor der eigentlichen Änderung in Schlüsselpaaren senden, und das System beim Benutzer wird die Änderung erst nach dem "gut ab" Datum implementieren. Und, natürlich, gibt das "gut bis" Datum 20 an, wann der Schlüssel abgelaufen ist. Auf diese Weise werden Benutzer nicht versehentlich Schlüssel in alten Notmeldungen verwenden.

[0029] Abschließend wird die digitale Unterschrift, welche die Zentralbehörde der Meldung anhängt, durch Verwendung des kompromittierten Wurzelschlüssels generiert.

Protokoll der Zentralbehörde

[0030] Unter Bezugnahme auf **Abb.** 2, wenn der Zentralbehörde ein Anzeichen vorliegt oder sie glaubt, dass ihr Wurzelschlüssel kompromittiert worden ist, selektiert sie ein neues, aus einem öffentlichen und einem privaten Schlüssel bestehendes, Ersatzschlüsselpaar und konstruiert eine Notmeldung zur Verteilung eines Ersatzschlüssels an Benutzer (Schritt 100). Sie konstruiert die Notmeldung durch Verketten der oben beschriebenen Information, einschließlich des Ersatzschlüssels, um ein Informationspaket zu generieren. Sie generiert danach eine digitale Unterschrift für jenes Informationspaket (Sehritt 102) und hängt die digitale Unterschrift an das Paket an, um die Notmeldung zu produzieren (Schritt 104).

[0031] Die Zentraleinheit verwendet den kompromittierten Wurzelschlüssel, um die digitale Unterschrift zu generieren. Die Unterschrift lässt sich auf verschiedene Arten generieren. Eine Art ist einen einer Anzahl bekannter digitaler Unterschriftsalgorithmen unter Verwendung des Wurzelschlüssels anzuwenden. Eine andere Art ist zuerst eine Einwegfunktion auf das Informationspaket anzuwenden, um eine kompaktere, Darstellung jener Information zu produzieren und danach den digitalen Unterschriftsalgorithmus mit dem Wurzelschlüssel zu verwenden.

[0032] Natürlich, falls letzterer Ansatz verwendet wird, muss dieselbe Einwegfunktion vom Empfänger der Notmeldung als Teil ihres Verifizierungsprozesses benutzt werden. Deshalb wird angenommen, dass die Einwegfunktion öffentlich verfügbar gemacht wird bzw. Eine weitläufig bekannte Einwegfunktion ist.

[0033] Sobald die digitale Unterschrift angehängt worden ist, um die komplette. Notmeldung zu produzieren, sendet sie die Zentralbehörde an andere Benutzer über Inbandkanäle, die sie typisch verwendet, um geschäftliche Kommunikation zu senden bzw. zu empfangen oder über speziell selektierte Inbandkanäle, die der Öffentlichkeit zugänglich sind (Schritt 106).

[0034] Die Zentralbehörde generiert und verteilt außerdem einen Verfizierungscode V, den Empfänger der Notmeldung verwenden können, um zu verifizieren, dass die Notmeldung legitim ist. Der Verfizierungscode wird durch Anwenden einer Einwegfunktion bzw. Einweg-Hash-Funktion auf die Notmeldung, oder einen Teil der Notmeldung generiert, um einen Hash-Wert zu generieren (Schritt 108). Die Einwegfunktion kann, angenommen, dass eine verwendet wurde, entweder mit der Einwegfunktion, die zum Generieren der digitalen Funktion benutzt wurde identisch bzw. von dieser verschieden sein.

[0035] In beiden Fällen stellt die Zentralbehörde die Einwegfunktion f(x) öffentlich zur Verfügung. Man sollte aber zur Kenntnis nehmen, dass in der Praxis. perfekte Einwegfunktionen möglicherweise eigentlich nicht existieren. Das heißt für alle Funktionen, die jetzt als Einwegfunktionen angesehen, werden, könnte schließlich genügend Rechenleistung oder Techniken zur Bestimmung von x_1, wenn $f(x_1)$ gegeben ist. Deshalb beabsichtigen wir mit der Phrase Einwegfunktion ebenso. jene Funktionen einzuschließen, für die es sehr schwierig, aber nicht notwendigerweise unmöglich, ist x1 durch Kennen von $f(x_1)$ zu berechnen.

[0036] Im beschriebenen Ausführungsbeispiel ist die Hash-Funktion der gut bekannte "Secure Hash Algorithm" /Sicherer Hash-Algorithmus (SHA). Die Einwegfunktion (en) kann/können jedoch eine beliebige einer Anzahl von Standard-Hash-Funktionen sein (z.B. MD5, SHA, usw.). Für eine Beschreibung des SHA und anderer akzeptabler Einweg-Hash-Funktionen wird der Leser auf die öffentliche Literatur hinsichtlich Kryptographie verwiesen, z.B. Angewandte Kryptographie von Bruce Schneier, herausgegeben von John Wiley & Sons, Inc.

[0037] Außerdem sollte weiter zur Kenntnis genommen werden, dass man mehrere Einwegfunktionen verwenden und diese verketten könnte. In dem Fachgebiet sind viele Einwegfunktionen bekannt und typisch sind viele davon leicht zu berechnen und sie lassen sich daher auf eine Chipkarte implementieren.

[0038] Nach Generieren des Verfizierungscode V veröffentlicht ihn die Zentralbehörde auf eine Weise, die seine Zuverlässigkeit sicherstellt, d. h. auf eine Weise, die Empfänger überzeugt, dass er tatsächlich von der Zentralbehörde stammt (Schritt 110). Dies wird das Verbreiten von V durch einen anderen Kommunikationskanal als den Kanal involvieren, der zum Senden der Notmeldung verwendet wurde (d. h. einen Außenbandkanal).

[0039] Es ist besonders wünschenswert, dass der Außenbandkanal ein Kanal ist, der nicht von einer dritten Partei übernommen bzw. Verfälscht werden kann, die den Wurzelschlüssel kompromittiert haben könnte: Der Außenbandkanal könnte eine gut bekannte (oder in eine Computeranwendung hartcodierte) 800-Nummer sein, die der Benutzer anrufen und den Hash-Wert dann telefonisch verifizieren kann. Oder es könnte vielleicht eine gut bekannte und vertrauenswürdige Veröffentlichung, wie beispielsweise eine nationale Zeitung oder Zeitschrift sein, in welcher der Verifizierungswert auf einer ge-

gebenen Seite an einem gegebenen Datum oder einem Bereich von Daten veröffentlicht wird. Die Verifizierung durch den Außenbandkanal des Hash-Werts V, den der Benutzer durch Anwenden der Einwegfunktion auf die Notmeldung produziert, gibt dem Benutzer einen hohen Grad an Zuversicht, dass die Notmeldung legitim ist, weil ein Widersacher den Außenbandkanal übernehmen oder mit diesem. Notmeldung zgemeinsame Sache machen müsste, um eine gültige u produzieren, was höchst unwahrscheinlich ist.

[0040] Der Vorteil des von uns beschriebenen Ansatzes ist, dass die Notmeldung durch jeden verbreitet werden kann. Die Zentralbehörde braucht keinen sofortigen Zugriff auf alle der zahlreichen Benutzer haben, die möglicherweise einen Ersatzschlüssel benötigen. Stattdessen kann sich die Zentralbehörde auf die anfänglichen Empfänger der Notmeldung verlassen (z.B. Kaufleute oder Verkäufer) sie an andere Benutzer (z.B. Verbraucher) weiterzuleiten. Tatsächlich ist ein Anreiz für Kaufleute vorhanden die Notmeldung an Verbraucher zu verbreiten, da der öffentliche Schlüssel der Zentralbehörde typisch erforderlich sein wird die Information zu beglaubigen, die während der geschäftlichen Transaktionen zwischen dem Verbraucher und dem Kaufmann ausgetauscht wird.

Öffentliches Benutzerprotokoll

[0041] Unter Bezugnahme auf **Abb.** 3, empfängt der Benutzer die Notmeldung elektronisch entweder direkt von der Zentralbehörde oder indirekt durch andere Mittler (Schritt 200). Nach Empfang der Notmeldung und deren Erkennen als eine Notmeldung, überprüft der Benutzer die "gut ab" und "gut bis" Daten in der. Meldung, um sicherzustellen, dass die Meldung aktuell ist (Schritt 202).

[0042] Angenommen, dass die Meldung aktuell ist, verifiziert der Benutzer dann die digitale Unterschrift, die Teil der Notmeldung ist (Schritt 204). Der Benutzer nimmt dies vor, indem er einen öffentlichen Schlüsselalgorithmus unter Verwendung des kompromittierten Wurzelschlüssels benutzt. Falls, die Zentralbehörde mehrfache Wurzelschlüssel verwendet, identifiziert der Benutzer den relevanten jener Schlüssel durch Untersuchung der Seriennummer in der Notmeldung.

[0043] Nach Bestimmen, dass die Notmeldung aktuell ist und deren . Beglaubigen, erhält der Benutzer dann den Verifizierungswert V von der Außenbandquelle (Schritt 206). Anschließend wendet der Benutzer die Einwegfunktion auf den entsprechenden Teil oder die ganze Notmeldung an, um einen weiteren Wert B (Schritt 208) zu generieren und vergleicht diesen mit dem vom Außenbandkanal erhaltenen Verifizierungswert V (Schritt 210). Wenn B gleich V ist, verifiziert dies, das die Notmeldung von der Zentralbehörde und nicht von irgendeiner Partei gesendet wurde, die sich den originalen Wurzelschlüssel, ohne Autorität ihn zu besitzen, verschafft hat. Es ist wichtig, dass der Benutzer B generiert, um zu verifizieren, dass es sich um einen korrekten und legitimen Wert handelt, da ein kompromittierter Schlüssel einem Gauner gestatten wird seine eigene Notmeldung in einem Versuch auszusenden die Kontrolle des Systems zu übernehmen.

[0044] Wenn der Benutzer verifiziert, dass V gleich B ist, dann ersetzt der Benutzer den alten öffentlichen Schlüssel mit dem in der Notmeldung enthaltenen Ersatzschlüssel (Schritt 212).

[0045] Falls an irgendeinem Punkt bei dieser Prozedur ein Test erfolglos ist, so ignoriert der Benutzer die Notmeldung und fährt fort den originalen öffentlichen Schlüssel zu benutzen, der dem orignalen Wurzelschlüssel entspricht. Natürlich, wenn der Benutzer feststellt, dass V nicht B gleicht, so weiß der Benutzer, dass es höchst wahrscheinlich ist, dass der Wurzelschlüssel kompromittiert worden ist, dass aber die Notmeldung ein Angriff auf das System durch die Partei war, die den Wurzelschlüssel kompromittiert hat.

[0046] Es dürfte offenkundig sein, dass Unterzeichnen der Notmeldung mit einem kompromittierten Wurzelschlüssel, in der Tat, einen wichtigen Schritt darstellt, selbst wenn der Wurzelschlüssel kompromittiert worden ist. Diese Unterschrift dient als eine erste Verteidigungslinie. Sie stellt sicher, dass nicht jeder einfach eine Notmeldung herausgeben kann, die den normalen Betrieb des Systems stört. Die Unterschrift bedeutet, dass die Notmeldung nur eine von zwei Quellen haben könnte, nämlich, die Systembehörde, die den Wurzelauthentifikationsschlüssel besitzt bzw. die Entität, die den Wurzelautehntifikationsschlüssel kompromittiert hat. Dieses reduziert die Anzahl der Entitäten erheblich, die eine Notmeldung verwenden könnten, um das System zu untergraben. Es sollte anerkannt werden, dass die Prozeduren für die Verarbeitung einer Notmeldung automatisch im Namen des Benutzers durch eine Rechenvorrichtung (z.B. einem PC-Computer) beim Benutzer vorgenommen können. Mit. Bezugnahme auf die **Abb.** 4 schließt der Computer typisch einen programmierbaren Prozessor 400 mit einer Kommunikationsschnittstelle 4,02 (z.B. ein Modem) zum Empfangen der Notmeldung über ein Kommunikationsglied 403, z.B. die Telefonleitungen, ein. Der Computer schließt außerdem einen Speicher 404, einschließlich Haupt- und Hilfsspeicher, zum Speichern der vom Benutzer benötigten öffentlichen Schlüssel und zum Speichern der Programme, die jene Schlüssel benutzen, einschließlich des Programms das die Notmeldung verarbeitet, ein. Das die Notmeldung verarbeitende Programm könnte ab anderen externen maschinenlesbaren Medien, wie beispielsweise einer Computerplatte 408, geladen werden. Der Computer schließt außerdem ein Eingabegerät 406 (z.B. eine Tastatur) ein, die dem Benutzer ermöglicht den Verfizierungscode einzugeben; der vom. Außenbandkanal wiedergewonnen wird, und ein Anzeigegerät (z.B. Video-

bildschirm) das dem Benutzer relevante Informationen anzeigt.

[0047] Der Computer empfängt die Notmeldung über die Kommunikationsverbindung und ist programmiert sie als eine Notmeldung zu erkennen. Er führt danach die oben beschriebenen Vorgänge aus. Dies könnte vollautomatisch geschehen oder Benutzersteuerung und -eingabe erfordern. Jedenfalls, angenommen, dass sich die Meldung als aktuelle erweist und den ersten Test ihrer Gültigkeit besteht d. h., die digitale Unterschrift wurde vom kompromittierten Wurzelschlüssel generiert), benachrichtigt der Computer dann den Benutzer einen Verfizierungscode zur Beglaubigung des neuen Schlüssels einzugeben. Beispielsweise könnte der Computer einen Dialogkasten am Bildschirm anzeigen, der sagt "nehmen Sie die NYTimes zur Hand und geben Sie die Nummer ein, die auf Seite x an dem und dem Datum veröffentlicht wurde" oder "Rufen Sie 1-800-Nummer an und tippen Sie die Nummer ein, die Ihnen vorgelesen wird". Mit anderen Worten , der Computer ersucht um Eingabe (d. h., die Verifizierungsnummer oder Kette), die von einer spezifizierten Außenbandkommunikation erhältlich ist.

[0048] Wenn der vom Benutzer eingegebene Verfizierungscode die Notmeldung verifiziert, dann würde der Computer den kompromittierten Schlüssel im Speicher mit dem neuen Ersatzschlüssel ersetzen.

[0049] Obwohl wir einen PC als Beispiel verwendet haben, kann die Rechenvorrichtung ein beliebiges einer großen Vielfalt elektronischer Geräte sein, die einen digitalen Prozessor, einschließlich, beispielsweise, einem PDI , einer Cipkarte, einem Slate-PC oder eine viel leistungsfähigere Arbeitsstation, einschließen, um nur einige zu nennen. Außerdem können die Kommunikationsmedien, über die die Übertragungen von Informationen stattfinden, ebenso eine. beliebige einer großer Zahl von Möglichkeiten, einschließlich, beispielsweise, Telefonleitungen, Telegramm, das Internet, Satellitenübertragungen oder Funkübertragungen sein. Mit anderen Worten, es ist nicht beabsichtigt, dass die Erfindung im Hinblick auf entweder die eingesetzten Gerätearten oder die zur Verwendung kommenden Kommunikationsmethoden eingeschränkt wird.

[0050] Es sollte natürlich ebenso verstanden sein, dass die Rechenvorrichtungen, entweder intern oder extern, alle Speicherkapazität, die für die Daten und bei der Implementierung der Protokolle erforderlichen Programme notwendig ist, ein schließen. Außerdem schließen sie jedwede Geräte (z. B. ein Modem) ein, die sie zur Kommunikation mit anderen Rechengeräten benötigen. Außerdem können die Kommunikationsmedien, über die die Übertragungen von Informationen stattfinden, ebenso eine beliebige einer großer $_{Z}$ahl von Möglichkeiten, einschließlich, beispielsweise, Telefonleitungen, Telegramm, das Internet, Satellitenübertragungen oder Funkübertragungen sein. Mit anderen Worten, es ist nicht beabsichtigt, dass die Erfindung im Hinblick auf entweder die eingesetzten Gerätearten, die zum Implementieren der oben beschriebenen Protokolle verwendet oder die zur Verwendung kommenden Kommunikationsmethoden eingeschränkt wird.

[0051] Andere Ausführungsbeispiele sind in den folgenden Ansprüchen enthalten.

[0052] Was beansprucht wird, ist:

Patentansprüche

1. Reaktionsverfahren auf eine Änderung eines Wurzelschlüssels, wobei besagter Wurzelschlüssel ein privater Schlüssel eines ersten, aus einem öffentlichen und einem privaten Schlüssel bestehenden, Schlüsselpaars ist, wobei besagtes Verfahren **dadurch gekennzeichnet** ist, das es folgende Schritte umfasst:

elektronischen Empfang (200) einer Meldung (10) durch einen Inbandkanal, wobei die besagte Meldung anzeigt, dass der Wurzelschlüssel ersetzt wird, die besagte Meldung außerdem einen Ersatzschlüssel (16) und eine digitale Unterschrift (22) enthält, die durch Verwendung des Wurzelschlüssels generiert wurde, besagter Ersatzschlüssel (16) ein öffentlicher Schlüssel eines zweiten, aus einem öffentlichen und einem privaten Schlüssel bestehenden, Schlüsselpaars ist, das das erste, aus einem öffentlichen und einem privaten Schlüssel bestehende, Schlüsselpaar ersetzt;

Verwendung (204) des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht, um die digitale Unterschrift der Meldung zu verifizieren;

Erhalten (206), durch einen Außenbandkanal, der vom Inbandkanal verschieden ist, eines Verifikations-Codewerts, V, der von der Meldung, durch Anwendung einer Einwegfunktion auf wenigstens einen Teil der Meldung, hergeleitet wurde;

Anwendung (208) der Einwegfunktion auf den besagten wenigstens einen Teil der Meldung, um einen Wert B zu generieren;

Vergleichen (210) von B mit V; und

falls B gleich V ist, Ersetzen (212) des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht, mit dem Ersatzschlüssel.

2. Das Verfahren des Anspruchs 1, bei dem die Meldung (10) eine Notmeldung umfasst, die anzeigt, dass der Wurzelschlüssel kompromittiert worden ist.

3. Das Verfahren des Anspruchs 2, das weiter den Schritt der Generierung der Meldung (10) durch Verketten des Ersatzschlüssels mit einer Kennung (12) umfasst, wobei die besagte Kennung die Meldung als eine Meldung identifiziert, die einen Ersatzschlüssel (16) trägt.

4. Das Verfahren des Anspruchs 2, das weiter den Schritt der Generierung der Meldung (10) durch Verketten des Ersatzschlüssels mit einer Seriennummer (14) umfasst, wobei die besagte Seriennummer

anzeigt welcher einer Vielheit von Wurzelschlüsseln ersetzt wird.

5. Das Verfahren des Anspruchs 2, das weiter den Schritt der Generierung der Meldung (10) durch Verketten des Ersatzschlüssels (16) mit einem "gut bis" Datum (20), das anzeigt wann der Ersatzschlüssel ablaufen wird.

6. Das Verfahren des Anspruchs 2, das weiter den Schritt der Generierung der Meldung (10) durch Verketten des Ersatzschlüssels mit einem "gut ab" Datum (18), das anzeigt wann der Ersatzschlüssel (16) aktiv werden wird.

7. Vorrichtung zum Reagieren auf eine Änderung eines Wurzelschlüssels, wobei besagter Wurzelschlüssel ein privater Schlüssel eines ersten, aus einem öffentlichen und einem privaten Schlüssel bestehenden, Schlüsselpaars ist, und besagte Vorrichtung umfasst:
einen Prozessor (400);
eine an besagten Prozessor angeschlossene Kommunikations-schnittstelle (402):
einen Speicher (404), der an besagten Prozessor (400) angeschlossen ist, und darin computer-ausführbare Instruktionen zur Ausführung durch den Prozessor speichert und außerdem den öffentlichen Schlüssel speichert, der dem Wurzelschlüssel entspricht; und
eine Eingabeeinrichtung (406), die an besagten Prozessor angeschlossen ist,
besagte Vorrichtung dadurch gekennzeichnet ist, dass:
durch besagte Kommunikationsschnittstelle (402), die an besagten Prozessor (400) angeschlossen ist, eine Meldung (10) elektronisch durch einen Inbandkanal empfangen wird, wobei die besagte Meldung anzeigt, dass der Wurzelschlüssel ersetzt wird, besagte Meldung außerdem einen Ersatzschlüssel (16) und eine digitale Unterschrift (22) enthält, die durch Verwendung des Wurzelschlüssels generiert wurde, besagter Ersatzschlüssel (16) ein öffentlicher Schlüssel eines zweiten, aus einem öffentlichen und einem privaten Schlüssel bestehenden, Schlüsselpaars ist, das das erste, aus einem öffentlichen und einem privaten Schlüssel bestehende, Schlüsselpaar ersetzt, und
durch besagte Eingabeeinrichtung (406), die an den Prozessor angeschlossen ist, ein Verifikations-Codewert V durch einen vom Inbandkanal verschiedenen Außenbandkanal eingegeben wird;
und, wobei der besagte Prozessor (400) als Antwort auf die Ausführung der Instruktionen:
den öffentlichen Schlüssel, der dem Wurzelschlüssel entspricht, dazu zu verwendet die digitale Unterschrift (204) der Meldung zu verifizieren;
durch den Außenbandkanal, den (206 Verifikations-Codewert, V, erhält, der, durch Anwendung einer Einwegfunktion auf wenigstens einen Teil der Meldung, von der Meldung hergeleitet wurde;
die (208) Einwegfunktion auf besagten wenigstens einen Teil der Meldung anwendet, um einen Wert B zu generieren;
B (210) mit V vergleicht; und
Falls B ist gleich V, den (212) öffentlichen Schlüssel, der dem Wurzelschlüssel entspricht, mit dem Ersatzschlüssel ersetzt.

8. Vorrichtung des Anspruchs 7, in dem die Meldung (10) eine Notmeldung umfasst, die anzeigt, dass der Wurzelschlüssel kompromittiert worden ist.

9. Vorrichtung des Anspruchs 8, in dem der Prozessor (400), als Antwort auf die Ausführung der Instruktionen, die Meldung durch Verketten des Ersatzschlüssels (16) mit einer Kennung (12)generiert, und besagte Kennung die Meldung als eine Meldung identifiziert, die einen Ersatzschlüssel trägt.

10. Vorrichtung des Anspruchs 8, in dem der Prozessor (400), als Antwort auf die Instruktionen, die Meldung durch Verketten des Ersatzschlüssels (16) mit einer Seriennummer (14) generiert, und die besagte Seriennummer anzeigt, welcher einer Vielheit von Wurzelschlüsseln ersetzt wird.

11. Vorrichtung des Anspruchs 8, in dem der Prozessor (400) als Antwort auf die Ausführung der Instruktionen, die Meldung durch Verketten des Ersatzschlüssels (16) mit einem "gut bis" Datum (20) generiert, das anzeigt, wann der Ersatzschlüssel ablaufen wird.

12. Vorrichtung des Anspruchs 8, in dem der Prozessor (400) als Antwort auf die Ausführung der Instruktionen, die Meldung durch Verketten des Ersatzschlüssels (16) mit einem "gut ab" Datum (18) generiert, das anzeigt, wann der Ersatzschlüssel aktiv werden wird.

13. Maschinenlesbarer Datenträger, der ein Computerprogramm (408) speichert, das auf einem Computer , der einschließt: einen Speicher, das Computerprogramm zur Reaktion auf eine Änderung eines Wurzelschlüssels, wobei der Wurzelschlüssel ein privater Schlüssel eines ersten, aus einem öffentlichen und privaten Schlüssel bestehenden, Schlüsselpaars ist, und besagtes gespeichertes Computerprogramm gekennzeichnet ist, indem es umfasst:
Maschinenlesbare Instruktionen, die bewirken, dass der Computer elektronisch (200) eine Meldung (10) durch einen Inbandkanal empfängt, wobei die besagte Meldung anzeigt, dass der Wurzelschlüssel ersetzt wird, und die besagte Meldung außerdem einen Ersatzschlüssel (16) und eine digitale Unterschrift (22) enthält, die durch Verwendung des Wurzelschlüssels generiert wurde, und der besagte Ersatzschlüssel (16) ein öffentlicher Schlüssel eines zweiten, aus einem öffentlichen und privaten Schlüssel bestehen-

den, Schlüsselpaars ist, das das erste, aus einem öffentlichen und privaten Schlüssel bestehende, Schlüsselpaar ersetzt.
Maschinenlesbare Instruktionen zum Erhalt (206), durch einen vom Inbandkanal verschiedenen Außenkanal, eines Verifikationswerts, V, der, durch Anwendung einer Einwegfunktion auf wenigstens einen Teil der Meldung, von der Meldung hergeleitet wurde;
Maschinenlesbare Instruktionen zum Vergleichen (210) von B mit V; und
Maschinenlesbare Instruktionen zum Ersetzen (212) des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht, mit dem Ersatzschlüssel, falls B ist gleich V.

14. Computerprogramm, das auf einem Computer ausführbar ist, der einen Speicher, das Computerprogramm zum Reagieren auf eine Änderung eines Wurzelschlüssels, einschließt, wobei der Wurzelschlüssel ein privater Schlüssel eines ersten, aus einem öffentlichen und privaten Schlüssel bestehenden, Schlüsselpaars ist, und das besagte Computerprogramm dadurch gekennzeichnet ist, dass es enthält:
Maschinenlesbare Instruktionen, die bewirken, dass der Computer elektronisch (200) eine Meldung (10) durch einen Inbandkanal empfängt, wobei die besagte Meldung anzeigt, dass der Wurzelschlüssel ersetzt wird, und die besagte Meldung außerdem einen Ersatzschlüssel (16) und eine digitale Unterschrift (22) enthält, die durch Verwendung des Wurzelschlüssels generiert wurde, und der besagte Ersatzschlüssel (16) ein öffentlicher Schlüssel eines zweiten, aus einem öffentlichen und einem privaten Schlüsel bestehenden, Schlüsselpaars ist, das das erste, aus einem öffentlichen und privaten Schlüssels bestehende, Schlüsselpaar ersetzt.
Maschinenlesbare Instruktionen zur Verwendung (202) des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht, um die digitale Unterschrift der Meldung zu verifizieren;
Maschinenlesbare Instruktionen zum Erhalt (206), durch einen vom Inbandkanal verschiedenen Außenkanal, eines Verifikationswerts, V, der, durch Anwendung einer Einwegfunktion auf wenigstens einen Teil der Meldung, von der Meldung hergeleitet wurde;
Maschinenlesbare Instruktionen zum Anwenden (208) einer Einwegfunktion auf wenigstens einen Teil der Meldung, um einen Wert B zu generieren;
Maschinenlesbare Instruktionen zum Vergleichen (210) von B mit V; und
Maschinenlesbare Instruktionen zum Ersetzen (212) des öffentlichen Schlüssels, der dem Wurzelschlüssel entspricht, mit dem Ersatzschlüssel, falls B ist gleich V.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

