(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2005 026 943 B4** 2009.01.29

(12) **Patentschrift**

(21) Aktenzeichen: **10 2005 026 943.5**
(22) Anmeldetag: **06.06.2005**
(43) Offenlegungstag: **22.12.2005**
(45) Veröffentlichungstag der Patenterteilung: **29.01.2009**

(51) Int Cl.[8]: ***H04L 9/28*** (2006.01)

(30) Unionspriorität:
10/862,286 07.06.2004 US

(73) Patentinhaber:
Rockwell Electronic Commerce Corp., Wood Dale, Ill., US

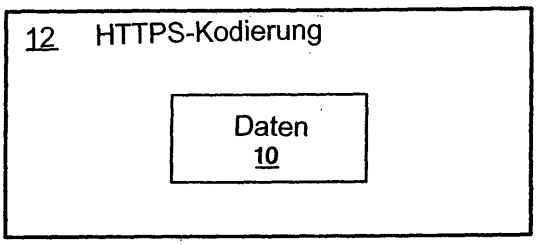
(74) Vertreter:
Wablat, W., Dipl.-Chem. Dr.-Ing. Dr.jur., Pat.-Anw., 14129 Berlin

(72) Erfinder:
Dezonno, Anthony, Bloomingdale, Ill., US

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2002/01 29 247 A1
US 53 15 658 A
US 52 31 668 A
US 52 14 703 A
US 51 40 634 A
US 48 50 017 A
US 47 48 668 A
US 44 05 829 A
US 42 18 582 A
US 42 00 770 A
US 39 62 539 A
WO 01/08 350 A1

(54) Bezeichnung: **Verfahren und System zur sicheren Kundenkommunikation**

(57) Hauptanspruch: Verfahren zur Einbeziehung von Kundenkodierung auf einem Kommunikationskanal zwischen einem Benutzer und einem Web-Server, wenn die Sicherheit des Kommunikationskanals als verletzt oder gefährdet ermittelt wurde, das aus folgenden Schritten besteht:
Einrichten eines Kundenkodierungssystems unter Verwendung eines Verschlüsselungsverfahrens zwischen einem Benutzer und einem Web-Server, wobei die Kundenkodierung das Einrichten eines Benutzernamens umfasst und der Kundencode zur Einrichtung von zwei (2) Kommunikationsschlüsseln für das Verschlüsselungsverfahren verwendet wird und die Kommunikationsverschlüsselungscodes als die beiden (2) größten Primzahlen der Kundenkontonummer definiert sind;
Ermitteln, ob die Sicherheit auf dem Kommunikationskanal gefährdet oder verletzt wurde;
Ermitteln, ob der Kunde fortfahren möchte;
Kommunizieren zwischen Benutzer und Web-Server über den Einsatz zusätzlicher Kundenkodierung in der weiteren Kommunikation über den Kommunikationskanal;
Auffordern des Benutzers zur Eingabe des Benutzernamens;
Auffordern des Benutzer zur Eingabe der Kundenkontonummer;
Speichern der Kundenkontonummer auf dem Computer des Benutzers und auf dem Web-Server;
Erstellen der Kommunikationsschlüssel und...



Beschreibung

Hintergrund der Erfindung

1. Sachgebiet

[0001] Die vorliegende Erfindung betrifft im Allgemeinen Kodierverfahren und im Besonderen Verfahren zur Gewährleistung einer sicheren Kommunikationsverbindung bei e-Commerce-Transaktionen.

2. Stand der Technik

[0002] Sichere Kommunikation ist von größter Wichtigkeit für den kommerziellen Erfolg elektronischer e-Commerce-Transaktionen. Der moderne Internet-Handel gründet sich auf die Annahme, dass sensible finanzielle und persönliche Daten verschlüsselt werden können, um die unbefugte Offenlegung über ein normales Netz zu verhindern. Dies geschieht üblicherweise mit einem als "HTTPS" oder Hyper Text Transfer Protocol Secure bekannten Verschlüsselungsstandard. Das HTTPS-Protokoll wurde für den Web-Server des Unternehmens ausgewählt, um zu gewährleisten, dass die Kommunikation mit einem Benutzer oder Web-Browser durch Verschlüsselung der über den Kanal gesendeten Daten gesichert wird. Dieser Standard übermittelt Daten, die sowohl beim Sender als auch beim Empfänger ver- und entschlüsselt werden, wozu zwischen Sender und Empfänger zugewiesene Schlüssel verwendet werden. Die Verwaltung dieser Schlüssel erfolgt normalerweise durch einen zentralen Registraturdienst, wie er zum Beispiel von RSA Security zur Verwaltung der Verteilung von Sicherheitskanalschlüsseln angeboten wird.

[0003] Es ist wohlbekannt, dass Primzahlen von mehreren Verschlüsselungsstandards als Schlüssel in der elektronischen Kommunikation verwendet werden. Zwei miteinander multiplizierte Primzahlen ergeben eine zerlegbare Zahl, deren einzige beiden Faktoren die beiden Primzahlen sind. Beide Primzahlen können dann Schlüssel einer verschlüsselten Nachricht in Verfahren wie dem RSA-Algorithmus werden. Die Verschlüsselungslänge in Schlüsselstandards liegt heute bei 1024 Bit, doch wird erwartet, dass diese Verschlüsselungsgröße mit größeren Speicherkapazitäten und Prozessorgeschwindigkeiten zu längeren Schlüsseln führen wird. Die Sicherheit der Transaktion basiert jedoch auf der Annahme, dass der Kommunikationskanal sicher ist.

[0004] Im Falle einer Gefährdung des sicheren HTTPS-Kanals wird dem Endbenutzer nur wenig Schutz geboten, zum Beispiel bei einer Internet-Transaktion mit einem Unternehmen, um mit diesem Unternehmen sicher zu kommunizieren. Wenn der Kommunikationskanal nicht sicher ist, kann die Übermittlung von Finanzdaten wie Angaben zur Kreditkarte zu einer unbeabsichtigten Offenlegung dieser Daten gegenüber anderen führen.

[0005] Früher hat man sich dabei auf den Einsatz eines auf einem einzigen Standard beruhenden Kommunikationsverfahrens verlassen. Bei solchen Lösungen kann die elektronische Sitzung Angriffen oder Betrugsversuchen ausgesetzt sein, wenn der Kodieralgorithmus öffentlich bekannt wird.

[0006] Eine weitere verbreitete Lösungstechnik ist die Erhöhung der Schlüsselgröße, wenn der Algorithmus eines Schlüsselcodes entdeckt wird.

[0007] Zu den US-Patenten, in denen Verschlüsselungstechniken des Standes der Technik offengelegt wurden, zählen unter anderem:

PATENT	PATENTINHABER/ IN
3,962,539	Ehrsam et al.
4,200,770	Hellman et al.
4,218,582	Hellman et al.
4,405,829	Rivest et al.
4,748,668	Shamir et al.
4,850,017	Matyas et al.
5,140,634	Guillou et al.
5,214,703	Lai et al.:
5,231,668	Kravitz
5,315,658	Micali

Kurzdarstellung

[0008] Bei einer erfindungsgemäßen Ausführungsform wird ein Verfahren zur Einrichtung eines sicheren Kanals oder einer Sicherheitsstufe während einer Internet-Transaktion bereitgestellt, nachdem eine Sicherheitsverletzung des Kanals entdeckt wurde (d. h. der Kanal nicht mehr sicher ist). Auf diese Weise kann der Benutzer/Browser weiterhin mit dem Server, zum Beispiel einer Bank, kommunizieren, während eine Sicherheitsstufe, nämlich kundenkodierte Sicherheit, aufgerufen wird.

[0009] Bei einer weiteren erfindungsgemäßen Ausführungsform wird ein Verfahren zum Erstellen von Kundenkommunikationsschlüsseln zur Nutzung über einen Kommunikationskanal bereitgestellt, das folgende Schritte umfasst: Wahl einer Codenummer, Wahl der beiden höchsten Primzahlen außer 1 und der Codenummer selbst, Ermittlung in der Codenummer, ob die einzelnen Primzahlen größer als die Quadratwurzel aus der Codenummer sind, und wenn das der Fall ist, Einrichten der beiden Kommunikationsschlüssel mit einem Web-Server.

[0010] Bei einer weiteren erfindungsgemäßen Ausführungsform wird ein Verfahren zum Aktivieren der Kundenkodierung auf einem Kommunikationskanal zwischen Benutzer und Web-Server bereitgestellt, wenn eine Sicherheitsverletzung oder -gefährdung auf dem Kanal bemerkt wurde, das folgende Schritte umfasst: Einrichten eines Kundenkodiersystems mit einem Verschlüsselungsverfahren zwischen Benutzer oder Web-Browser/Benutzer und einem Web-Server, wobei die Kundenkodierung weiterhin die Einrichtung eines Benutzernamens und die Verwendung des Kundencodes für das Einrichten zweier (2) Kommunikationsschlüssel für das Verschlüsselungsverfahren umfasst und die beiden Kommunikationsschlüssel durch die zwei (2) größten Primzahlen der Kundenkontonummer definiert werden; Ermittlung, ob die Sicherheit des Kommunikationskanals gefährdet oder verletzt wurde; Ermittlung, ob der Kunde fortfahren möchte; Kommunikation zwischen Kunden/Web-Browser und dem Web-Server darüber, dass bei weiterer Kommunikation über diesen Kanal zusätzliche Kundenkodierung eingesetzt wird; Auffordern des Benutzers oder Web-Browsers zur Angabe des Benutzernamens; Aufforderung an den Kunden zur Eingabe der Kundenkontonummer; Speichern der Kundenkontonummer auf dem Computer des Kunden und auf dem Web-Server; Erstellen von Kommunikationsschlüsseln und Fortsetzung des Transfers von kundenkodierten Nachrichten über den Kommunikationskanal, bis die Kommunikation beendet ist.

Kurzbeschreibung der Zechnungsansichten

[0011] Ein besseres Verständnis der Erfindung und ihrer Vorzüge soll unter Bezugnahme auf die folgende Beschreibung und die beigefügten Figuren, die einige Ausführungsbeispiele der Erfindung zeigen, erzielt werden.

[0012] Fig. 1 zeigt ein Blockdiagramm der Standardverschlüsselung mit HTTPS (Hyper Text Transfer Protocol Secure) nach dem Stand der Technik.

[0013] Fig. 2 zeigt ein Blockdiagramm der Standardverschlüsselung von Kundendaten mit HTTPS (Hyper Text Transfer Protocol Secure) und Kundenkodierung der Daten nach einer erfindungsgemäßen Ausführungsform.

[0014] Fig. 3 zeigt eine Tabelle eines Beispiels der Kundenkodierung mit Kundenkennung oder Benutzernamen, Kundenkontonummer (Telefonnummer), Anzahl der Faktoren, den Primzahlenfaktoren und der Quadratwurzel aus Kontonummer oder Kontocode.

[0015] Fig. 4 zeigt ein Flussdiagramm einer Ausführungsform der bei der Kundenkodierung durchgeführten Schritte.

[0016] Während die vorliegende Erfindung für eine Reihe von verschiedenen Ausführungsformen geeignet ist, zeigen die Zeichnungen und die zugehörende Beschreibung nur einige Ausführungsbeispiele ohne Einschränkungscharakter, so dass diese Offenlegung lediglich ein Beispiel der Erfindung umfasst und keine Beschränkung der Erfindung auf die dargestellten Ausführungsformen bedeutet. In dieser Offenlegung soll der Gebrauch des Disjunktivs den Konjunktiv einschließen. Der Gebrauch des bestimmten oder unbestimmten Artikels soll keine Kardinalität anzeigen. Insbesondere soll der Bezug auf "das" oder "ein" Objekt auch die mögliche Pluralität solcher Objekte bezeichnen.

[0017] RSA ist ein Internet-Verschlüsselungs- und -Authentifizierungssystem, das sich eines 1977 von Ron Rivest, Adi Shamir und Leonard Adleman entwickelten Algorithmus bedient. Der RSA-Algorithmus ist ein oft

genutzter Verschlüsselungs- und Authentifizierungsalgorithmus, der in die Web-Browser von Microsoft und Netscape integriert ist. Er ist auch Bestandteil von Lotus Notes, Intuits Quicken und vielen anderen Produkten. RSA Security besitzt Rechte an diesem bestimmten Verschlüsselungssystem. Das Unternehmen lizenziert die Algorithmustechnologien und verkauft auch Development-Kits. Die Technologien sind Teil von vorhandenen oder vorgeschlagenen Web-, Internet- und Computer-Normen.

[0018] Die mathematischen Details des zum Erhalt der öffentlichen und privaten Schlüssel genutzten Algorithmus sind auf der RSA-Website verfügbar. Kurz gesagt umfasst der Algorithmus die Multiplikation zweier großer Primzahlen (eine Primzahl ist eine Zahl, die sich nur durch sich selbst und durch 1 teilen lässt) und durch weitere Operationen die Herleitung einer Menge von zwei Zahlen, die einen öffentlichen Schlüssel, und einer weiteren Menge, die einen privaten Schlüssel darstellt. Nach Entwicklung der Schlüssel sind die ursprünglichen Primzahlen nicht mehr wichtig und können verworfen werden. Sowohl der öffentliche als auch der private Schlüssel sind zur Ver- und Entschlüsselung erforderlich, doch nur der Inhaber des privaten Schlüssels muss diesen je kennen. Mit dem RSA-System braucht der private Schlüssel nie über das Internet gesendet zu werden.

[0019] Der private Schlüssel dient zur Entschlüsselung von Text, der mit dem öffentlichen Schlüssel verschlüsselt wurde. Wenn eine Seite eine Nachricht übermitteln möchte, kann diese den öffentlichen Schlüssel (jedoch nicht den privaten Schlüssel) des Empfängers vom zentralen Administrator herausfinden und mit diesem öffentlichen Schlüssel eine Nachricht an die Empfängerseite verschlüsseln. Wird eine verschlüsselte Nachricht empfangen, so wird diese mit dem privaten Schlüssel der Empfängerseite entschlüsselt. Zusätzlich zum Verschlüsseln von Nachrichten (was Datenschutz gewährleistet) kann man sich gegenüber der Empfängerseite authentifizieren (so dass die Empfängerseite weiß, wer die Nachricht in Wirklichkeit gesendet hat), indem mit deren privatem Schlüssel ein digitales Zertifikat verschlüsselt wird. Wenn die Empfängerseite das digitale Zertifikat empfängt, kann sie es mit dem öffentlichen Schlüssel des Absenders entschlüsseln.

[0020] Ein Beispiel für die Einkapselung oder Überblendung der Kundenkodierung von Daten in einer HTTPS-Nachricht nach dem Stand der Technik ist in Fig. 1 dargestellt, worin die Daten mit **10** und das HTTPS mit **12** bezeichnet sind. Die dargestellte Ausführungsform in Fig. 1 nutzt ein vorabgestimmtes Protokoll zwischen Benutzer, Kunden oder Web-Browser und dem Server, der die Kundenkontodaten bzw. die zwischen Benutzer und Server vorabgestimmte Kundenkodierung verwendet.

[0021] Wenn kein sicherer Kanal vorhanden ist, ist die Kodierung durch den Kunden mit einer Kundenkodierung **14** in der in Fig. 2 dargestellten Ausführungsform realisierbar und kann den Benutzernamen des Kunden und ausgewählte Kundendaten wie eine Kontonummer oder Telefonnummer zur sekundären Verschlüsselung von Angaben umfassen, die normalerweise über einen gesicherten Kanal übertragen werden. Wenn kein sicherer Kanal vorhanden ist, kann der Benutzer zur Eingabe der Kontodaten in die Benutzer- oder Browser-Anwendung zur Erzeugung von Verschlüsselungscodes, die sowohl dem Benutzer/Kunden als auch dem Server/der Bank bekannt sind, aufgefordert werden.

[0022] Wenn sich der Verbraucher dem Web-Server mit einer öffentlichen Identität zu erkennen gibt, wird der Web-Benutzer dann aufgefordert, einen speziellen Identifikationscode über einen sicheren Kanal wie HTTPS einzugeben. Wird dabei festgestellt, dass der sichere Kanal nicht verfügbar ist, wird dem Benutzer die Möglichkeit gegeben, die Angaben als verschlüsselte Sitzung mit der Benutzerkontonummer als Abfrageantwort zu senden. Da die Kontonummer sowohl der Website (dem Server) als auch dem Benutzer, Verbraucher oder Web-Browser bekannt ist, ist dies ein Verfahren mit gemeinsamem Schlüssel, und der empfangende Web-Server dekodiert die Angaben vom Benutzer mit der Kontonummer des Benutzers als Entschlüsselungs-Zugriffsnummer. Folglich kann eine zusätzliche, für Kundendaten spezifische Einkapselung für jeden einzelnen Kunden eingesetzt werden, was einer feindlichen Umgebung die Entschlüsselung erschwert.

[0023] Als Benutzername kann der Benutzername des Kunden und als Kundenkontonummer die Telefonnummer des Kunden verwendet werden. Zum Erstellen der Verschlüsselungscodes ermittelt das System bei einer Ausführungsform die beiden größten Primzahlen der Kundenkontonummer, d. h. der Telefonnummer des Kunden, wobei die gewählten großen Primzahlen größer als die Quadratwurzel aus der Telefonnummer sind. Mit diesen beiden Primzahlen wird dann ein Verschlüsselungsverfahren wie RSA (Rivest, Shamir und Adleman-Verschlüsselungssystem), PGP (Pretty Good Privacy) oder DES (Data Encryption Standard Algorithm) eingesetzt.

[0024] Ein weiterer Vorzug dieser Umgebung besteht darin, dass der Schlüssel zwischen den Seiten nicht über das öffentliche Netz ausgetauscht zu werden braucht, da beide mit dem Schlüssel die zu sendende Nach-

richt kodieren können. Obwohl ein gemeinsamer Kennzeichnungscode wie die Telefonnummer verwendet wird, muss dieser jedoch nicht direkt als Code für das Verschlüsselungssystem genutzt werden. Bei Verwendung der Telefonnummer als Kontobeispiel können zusätzliche 22 Bit Verschlüsselungsstärke zur Nachrichtenkodierung auf dem Kommunikationspfad genutzt werden, indem auf der Grundlage der kundenspezifischen Angaben eine weitere Verschlüsselung erfolgt.

[0025] Fig. 3 ist eine Beispieltabelle mit folgenden Spalten: Eine Kundenkennung (z. B. eine Kunden-ID-Nr. oder ein Benutzername); ein Kuntenkontocode, hier die Telefonnummer des Kunden, die Anzahl der Faktoren in der Telefonnummer, die Faktoren, von denen einige Primzahlen sind, sowie die Quadratwurzel aus dem Kundenkontocode.

[0026] Bei Auswahl des gemeinsamen Schlüssels ist es bevorzugt, statt der Verwendung der Daten selbst als Schlüssel ein Verfahren zur Generierung des geeignetsten Schlüssels einzusetzen, auch wenn Kontendaten wie die Telefonnummer sowohl dem Benutzer als auch dem Unternehmen direkt bekannt sind. Der Schlüssel wird vor dem HTTPS-Fehler oder während der öffentlichen Informationssitzung vereinbart, wiewohl es wertvoll ist, die Schlüsselwahl zur Verhinderung möglicher Interpretation geheim zu halten. Daher werden in einer bevorzugten Ausführungsform die größten Primfaktoren in der Faktorliste als Schlüssel für die Kommunikation verwendet. Zudem kommen als Kandidaten für die Schlüsselauswahl nur Primfaktoren in Betracht, die größer als die Quadratwurzel (Quadratwurzelspalte angegeben) aus den gemeinsamen Daten in Betracht. Wenn die Kundendaten eine Primzahl (2 Faktoren) oder eine zerlegbare Zahl (mehr als 2 Faktoren) darstellen, ist es außerdem wünschenswert, eine vereinbarte Variante der Kundendaten wie die nächst höhere Zahl, die diese Bedingung nicht erfüllt, für die vereinbarten gemeinsamen Informationen zwischen Benutzer und Web-Server auszuwählen. Als Alternative kann ein vereinbarter Algorithmus auf die Kontonummer angewendet werden.

[0027] Ein Flussdiagramm, das eine Ausführungsform des Verfahrens für die Durchführung der Kodierung veranschaulicht, ist in Fig. 4 dargestellt. Nach dem Start des Web-Browsers entsprechend Block **30** lädt der Benutzer die URL-Liste der besuchten Sites, die HTTPS ausgeführt haben, und erfasst dann den aktuellen URL, auf den entsprechend **31**, **32** zugegriffen wird. In Block **33** wird dann ermittelt, ob der adressierte URL auf der letzten sicheren Zugangsliste steht. Mit anderen Worten, ist das HTTPS für diesen Kanal vom Benutzer zu einem Web-Server (wie der Website einer Bank) sicher, oder wurde es verletzt?

[0028] Danach wird ermittelt, ob das verletzte HTTPS dasjenige ist, das der in Block **34** gezeigte Web-Browser anzeigt. Lautet die Antwort "Ja", wird der Benutzer gefragt, ob die in Block **35** dargestellte zusätzliche Sicherheit gewünscht wird. An dieser Stelle kann der Benutzer wählen, ob die Sitzung beendet wird oder feststellen, ob das HTTPS gefährdet ist. Ist dies der Fall, kann er vom Web-Server/der Bank die in den Blocks **36**, **37** und **38** dargestellte zusätzliche Sicherheit anfordern. Auf dieser Prozess-Stufe ist die Art der Sicherheit, z. B. RSA, PGP, DES usw. bereits unter Verwendung der beiden höchsten Primzahlen des Kundenkontocodes/der Telefonnummer und von Zahlen größer als die Quadratwurzel aus der Telefonnummer bereits vorabgestimmt.

[0029] Wie Block **39** zeigt, informiert das Unterdienstprogramm (siehe Blocks **35**, **37** und **38**) und das Hauptdienstprogramm (siehe Block **34**) den Web-Server des Benutzers, dass der Kommunikationskanal nicht mehr sicher ist, d. h., das HTTPS wurde verletzt oder gefährdet. Der Web-Server fordert den Benutzer dann zur Eingabe des Namens oder der öffentlichen Kennung auf, und der Benutzer übermittelt den Benutzernamen entsprechend der Darstellung in Block **40**. Der Web-Server sendet dann das zuvor vereinbarte Verschlüsselungsverfahren zur Ausführung an den Benutzer oder Web-Browser, und der Benutzer wird aufgefordert, die vereinbarte Kontonummer bzw. Telefonnummer wie in Block **41**, **42** dargestellt einzugeben. Die Konto- oder Telefonnummer wird dann auf dem Computer des Benutzers gespeichert, und es werden entsprechend den Blocks **43**, **44** Kommunikationsschlüssel erstellt.

[0030] Zwischen Benutzer und Web-Server werden unter Verwendung der Kommunikationsschlüssel Nachrichten ausgetauscht, bis der Benutzer den URL ändert und die Kommunikation als abgeschlossen (siehe Block **45**, **46**).

[0031] Die speziellen Ausführungsformen der neuartigen Verfahren für sichere Kommunikation wurden zur beispielhaften Veranschaulichung der Erfindung angeführt und stellen keine Beschränkung der Erfindung auf die dargestellten Ausführungsformen dar. Zahlreiche Modifikationen und Varianten können ohne Abweichung vom Umfang des neuartigen Grundgedankens der Erfindung umgesetzt werden. Eine Beschränkung auf die spezifische dargestellte Ausführungsform ist weder beabsichtigt noch ableitbar. Somit decken die angemeldeten Ansprüche sämtliche in den Umfang der hier offen gelegten und beanspruchten Erfindung fallenden Aus-

führungsformen, Modifikationen, Varianten oder Äquivalente ab.

Bezugszeichenliste

Fig. 1 STAND DER TECHNIK

12 HTTPS-Kodierung

Fig. 2

12 HTTPS-Kodierung

Fig. 3 (Spalten von links nach rechts)

Kundenkennung
Kundenkontonummer (z. B. Telefonnummer)
Anzahl an Faktoren
Faktoren-Primzahlen
Quadratwurzel

Bezugszeichenliste

Fig. 4

30 Start des Web-Browsers
31 Laden der URL-Liste der besuchten Sites, die HTTPS ausgeführt haben
32 Erfassendes URL-Codes, auf den zugegriffen wird
33 Steht der aktuelle URL auf der letzten Liste sicherer Adressen?
34 Verwendet der Web-Browser HTTPS?
35 Benutzer fragen, ob zusätzliche Sicherheit erforderlich ist
36 ERLEDIGT
37 Ermitteln, ob HTTPS gefährdet ist
38 Anforderung zusätzlicher Sicherheit an Web-Server senden
39 Benutzer mitteilen, dass Kanal nicht mehr sicher ist
40 Benutzer nach öffentlicher Kennung fragen
41 Web-Server sendet Verschlüsselungsverfahren zur Ausführung an Web-Browser
42 Benutzer nach vereinbartem Kontocode fragen
43 Kontencode auf lokalem Computer speichern
44 Kommunikationsschlüssel erstellen
45 Mit diesen Schlüsseln Nachrichten zwischen Web-Server und Benutzer übertragen
46 Hat sich der URL im Web-Browser geändert?

Patentansprüche

1. Verfahren zur Einbeziehung von Kundenkodierung auf einem Kommunikationskanal zwischen einem Benutzer und einem Web-Server, wenn die Sicherheit des Kommunikationskanals als verletzt oder gefährdet ermittelt wurde, das aus folgenden Schritten besteht:
Einrichten eines Kundenkodierungssystems unter Verwendung eines Verschlüsselungsverfahrens zwischen einem Benutzer und einem Web-Server, wobei die Kundenkodierung das Einrichten eines Benutzernamens umfasst und der Kundencode zur Einrichtung von zwei (2) Kommunikationsschlüsseln für das Verschlüsselungsverfahren verwendet wird und die Kommunikationsverschlüsselungscodes als die beiden (2) größten Primzahlen der Kundenkontonummer definiert sind;
Ermitteln, ob die Sicherheit auf dem Kommunikationskanal gefährdet oder verletzt wurde;
Ermitteln, ob der Kunde fortfahren möchte;
Kommunizieren zwischen Benutzer und Web-Server über den Einsatz zusätzlicher Kundenkodierung in der weiteren Kommunikation über den Kommunikationskanal;
Auffordern des Benutzers zur Eingabe des Benutzernamens;
Auffordern des Benutzer zur Eingabe der Kundenkontonummer;
Speichern der Kundenkontonummer auf dem Computer des Benutzers und auf dem Web-Server;
Erstellen der Kommunikationsschlüssel und

Fortsetzen der Übertragung von kundenkodierten Nachrichten über den Kommunikationskanal bis zum Abschluss der Kommunikation.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Kommunikationskanal mit einer ersten Stufe von HTTPS-Verschlüsselung bereitgestellt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Verschlüsselungsverfahren aus den Algorithmen RSA, PGP oder DES ausgewählt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die genannten Kommunikationsschlüssel die zwei (2) größten Primzahlen in der Kundenkontonummer außer dieser Nummer selbst und der Zahl 1 sind.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kontencodenummer keine Zahl sein kann, deren eine der beiden größten Primzahlen kleiner als die Quadratwurzel aus dieser Kontencodenummer ist.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Codenummer die Telefonnummer des Benutzers ist, es sei denn, dass sich aus ihr keine zwei weiteren Primzahlen als die Nummer selbst und die Zahl 1 erhalten lassen.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die beiden Primzahlen beide größer als die Quadratwurzel aus der Telefonnummer sein müssen.

8. Verfahren zum Erstellen von Kommunikationsverschlüsselungscodes zur Verwendung über einen Kommunikationskanal, das folgende Schritte umfasst:
Auswahl einer Codenummer;
Wahl der beiden höchsten Primzahlen außer 1 und der Codenummer selbst, die sich in der Codenummer befinden;
Ermittlung, ob diese Primzahlen größer als die Quadratwurzel aus der Codenummer sind, und wenn dies der Fall ist,
Einrichten zweier Kommunikationsverschlüsselungscodes gleich den beiden höchsten Primzahlen mit einem Web-Server.

9. Verfahren nach Anspruch 8, bei dem die Codenummer die Telefonnummer des Benutzers ist.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass eine durch einen Algorithmus modifizierte Zahl gleich der Codenummer ausgewählt wird, wenn keine zwei Primzahlen aus der Codenummer erhalten werden können oder wenn eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus der Codenummer ist.

11. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass eine Zahl gleich der Codenummer ± n ausgewählt wird, wenn keine zwei Primzahlen aus der Codenummer erhalten werden können oder wenn eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus der Codenummer ist.

12. System zur Einbeziehung von Kundenkodierung auf einem Kommunikationskanal zwischen einem Benutzer und einem Web-Server, wenn die Sicherheit des Kommunikationskanals als verletzt oder gefährdet ermittelt wurde, das aus folgende Merkmale aufweist:
Kommunikationsausrüstung zum Einrichten eines Kundenkodiersystems zwischen einem Kunden und einem Web-Server unter Verwendung eines Verschlüsselungsverfahrens;
wobei die genannte Kommunikationsausrüstung in der Lage ist, zwei (2) Kommunikationsschlüssel für das Verschlüsselungsverfahren unter Einschluss eines Kunden-Benutzernamens und einer Kundenkontonummer einzurichten,
die Kommunikationsverschlüsselungscodes durch die zwei (2) größten Primzahlen der Kundenkontonummer definiert werden,
die genannte Kommunikationsausrüstung ermitteln kann, ob die Sicherheit auf dem Kommunikationskanal gefährdet oder verletzt wurde;
die genannte Kommunikationsausrüstung in der Lage ist, eine Anzeige des Benutzers zu übermitteln,
dass dieser trotz der Sicherheitsverletzung oder -gefährdung die Kommunikation auf dem Kommunikationskanal fortzusetzen wünscht;
die genannte Kommunikationsausrüstung in der Lage ist, zwischen Benutzer und Web-Server über den Ein-

satz zusätzlicher Kundenkodierung in der weiteren Kommunikation auf dem Kommunikationskanal zu kommunizieren;
die genannte Kommunikationsausrüstung den Benutzer dann auffordert, den Benutzernamen und die Benutzerkontonummer anzugeben;
die genannte Kommunikationsausrüstung die Kundenkontonummer dann auf dem Computer des Benutzers und auf dem Web-Server speichert, wonach sie die Kommunikationsschlüssel erstellt; und
die genannte Kommunikationsausrüstung die Übertragung von kundenkodierten Nachrichten über den Kommunikationskanal bis zum Abschluss der Kommunikation fortsetzt.

13. System nach Anspruch 12, dadurch gekennzeichnet, dass der Kommunikationskanal mit einer ersten Stufe von HTTPS-Verschlüsselung bereitgestellt wird.

14. System nach Anspruch 12, dadurch gekennzeichnet, dass das Verschlüsselungsverfahren aus den Algorithmen RSA, PGP oder DES ausgewählt wird.

15. System nach Anspruch 12, dadurch gekennzeichnet, dass die genannten Kommunikationsschlüssel die zwei (2) größten Primzahlen in der Kundenkontonummer außer dieser Nummer selbst und der Zahl 1 sind.

16. System nach Anspruch 12, dadurch gekennzeichnet, dass die Kontencodenummer keine Zahl sein kann, deren eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus dieser Kontencodenummer ist.

17. System nach Anspruch 12, dadurch gekennzeichnet, dass die Codenummer die Telefonnummer des Benutzers ist, es sei denn, dass sich aus ihr keine zwei weiteren Primzahlen als die Nummer selbst und die Zahl 1 erhalten lassen.

18. System nach Anspruch 17, dadurch gekennzeichnet, dass die zwei Primzahlen beide größer als die Quadratwurzel aus der Telefonnummer sein müssen.

19. System zum Erstellen von Kommunikationsverschlüsselungscodes zur Verwendung über einen Kommunikationskanal, das folgende Merkmale aufweist:
Kommunikationsausrüstung zur Auswahl einer Codenummer;
wobei die genannte Kommunikationsausrüstung die beiden höchsten Primzahlen außer 1 und der Codenummer selbst, die sich in der Codenummer befinden, wählt;
die genannte Kommunikationsausrüstung ermittelt, ob diese Primzahlen größer als die Quadratwurzel aus der Codenummer sind, und wenn dies der Fall ist, die genannte Kommunikationsausrüstung in der Lage ist, zwei Kommunikationsverschlüsselungscodes einzurichten, die gleich den zwei größten Primzahlen sind.

20. System nach Anspruch 19, bei dem die Codenummer die Telefonnummer des Benutzers ist.

21. System nach Anspruch 19, dadurch gekennzeichnet, dass eine durch einen Algorithmus modifizierte Zahl gleich der Codenummer ausgewählt wird, wenn keine zwei Primzahlen aus der Codenummer erhalten werden können oder wenn eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus der Codenummer ist.

22. System nach Anspruch 19, dadurch gekennzeichnet, dass eine Zahl gleich der Codenummer ± n ausgewählt wird, wenn keine zwei Primzahlen aus der Codenummer erhalten werden können oder wenn eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus der Codenummer ist.

23. System zum Empfangen von Kundenkodierung auf einem Kommunikationskanal zwischen einem Benutzer und einem Web-Server, wenn die Sicherheit des Kommunikationskanals als verletzt oder gefährdet ermittelt wurde, das aus folgende Merkmale aufweist:
Kommunikationsausrüstung zum Einrichten eines Kundenkodiersystems zwischen einem Kunden und einem Web-Server unter Verwendung eines Verschlüsselungsverfahrens;
wobei die genannte Kommunikationsausrüstung in der Lage ist, zwei (2) Kommunikationsschlüssel für das Verschlüsselungsverfahren unter Verwendung einer gewählten Kundenkennungskontonummer einzurichten, die Kommunikationsverschlüsselungscodes durch die zwei (2) größten Primzahlen der Kundenkontonummer definiert werden,
die genannte Kommunikationsausrüstung ermitteln kann, ob die Sicherheit auf dem Kommunikationskanal gefährdet oder verletzt wurde;

die genannte Kommunikationsausrüstung in der Lage ist, eine Anzeige des Benutzers zu übermitteln, dass dieser die Kommunikation auf dem Kommunikationskanal fortzusetzen wünscht;
die genannte Kommunikationsausrüstung in der Lage ist, dem Benutzer mitzuteilen, dass in der weiteren Kommunikation auf dem Kommunikationskanal zusätzliche Kundenkodierung eingesetzt wird;
die genannte Kommunikationsausrüstung den Benutzer dann zur Angabe eines Kundenkenncodes auffordert;
die genannte Kommunikationsausrüstung den Kundenkenncode vom Web-Server abruft und Kommunikationsschlüssel erstellt und
die genannte Kommunikationsausrüstung die Übertragung von kundenkodierten Nachrichten über den Kommunikationskanal bis zum Abschluss der Kommunikation fortsetzt.

24. System nach Anspruch 23, dadurch gekennzeichnet, dass der Kommunikationskanal mit einer ersten Stufe von HTTPS-Verschlüsselung bereitgestellt wird.

25. System nach Anspruch 23, dadurch gekennzeichnet, dass das Verschlüsselungsverfahren aus den Algorithmen RSA, PGP oder DES ausgewählt wird.

26. System nach Anspruch 23, dadurch gekennzeichnet, dass die genannten Kommunikationsschlüssel die zwei (2) größten Primzahlen in der Kundenkontonummer außer dieser Nummer selbst und der Zahl 1 sind.

27. System nach Anspruch 23, dadurch gekennzeichnet, dass die Kontencodenummer keine Zahl sein kann, deren eine der zwei größten Primzahlen kleiner als die Quadratwurzel aus dieser Kontencodenummer ist.

28. System nach Anspruch 23, dadurch gekennzeichnet, dass die Codenummer die Telefonnummer des Benutzers ist, es sei denn, dass sich aus ihr keine zwei weiteren Primzahlen als die Nummer selbst und die Zahl 1 erhalten lassen.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

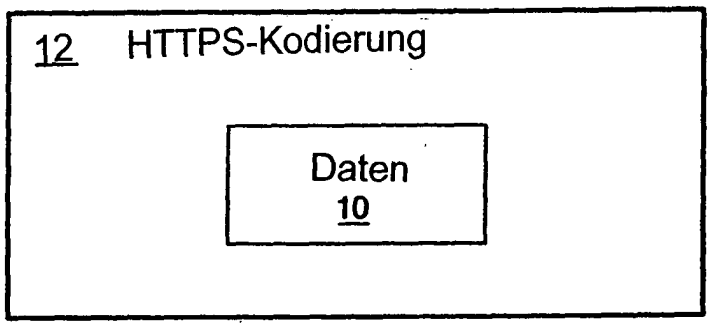


FIG. 1
STAND DER TECHNIK

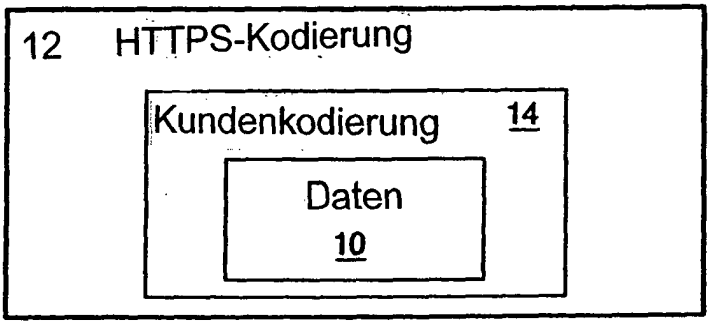


FIG. 2

Kunden-kennung	Kundenkonto-Nr. (z.B. Telefon-Nr.)	Anzahl an Faktoren	Faktoren – Primzahlen	Quadrat-wurzel
3272	2278057	2	191 11927	1509.3
3273	2278058	6	2 23 46 49523 99046 1139029	1509.3
3274	2278059	10	3 7 21 49 147 15497 46491 108479 325437 759353	1509.3
3275	2278060	10	2 4 5 10 20 113903 227806 455612 569515 1139030	1509.3
3276	2278061	2	149 15289	1509.3
3277	2278062	22	2 3 6 9 18 38 57 114 171 3426661 13322 19983 39966 59949 119898 126559 253118 379677 759354	
3278	2278063	0	1139031	1509.3
3279	2278064	18	0	1509.3
3280	2278065	6	2 4 8 16 176 346 692 623 1384 1646 2768 3292 6584 13168 142379 284758 569516 1139032	1509.3
3281	2278066	30	3 5 15 151871 455613 759355 2 7 14 29 31 58 62 181 203 217 362 406 434 899 1267 1798 2534 5249 5611 6293 10498 11222 12586 36743	1509.3
3282	2278067	10	39277 7386 78554 162719 325438 1139033	1509.3
3283	2278068	46	11 67 121 281 737 3091 8107 18827 34001 207097 2 3 4 6 12 13 17 26 34 39 51 52 68 78 102 156 204 221 442 663 659 884 1326 1718 2577 2652 3436 5154 10308 11167 14603 22334 29206 33501 43809 44668 58412 67002 87618 134004 175236 189839 379678	1509.3
3284	2278069	0	569517 759356 1139034	1509.3
3285	2278070	14	0	1509.3
3286	2278071	14	2 5 10 157 314 785 1451 1570 2902 7255 14510 227807 455614 1139035	1509.3
3287	2278072	6	3 9 27 139 417 607 1251 1821 3753 5463 16389 84373 253119 759357	1509.3
3288	2278073	2	2 4 8 284759 569518 1139036	1509.3
3289	2278074	6	7 325439	1509.3
3290	2278075	10	2 3 6 379679 759358 1139037	1509.3
			5 25 293 311 1465 1555 7325 7775 91123 455615	1509.3

FIG. 3

DE 10 2005 026 943 B4 2009.01.29

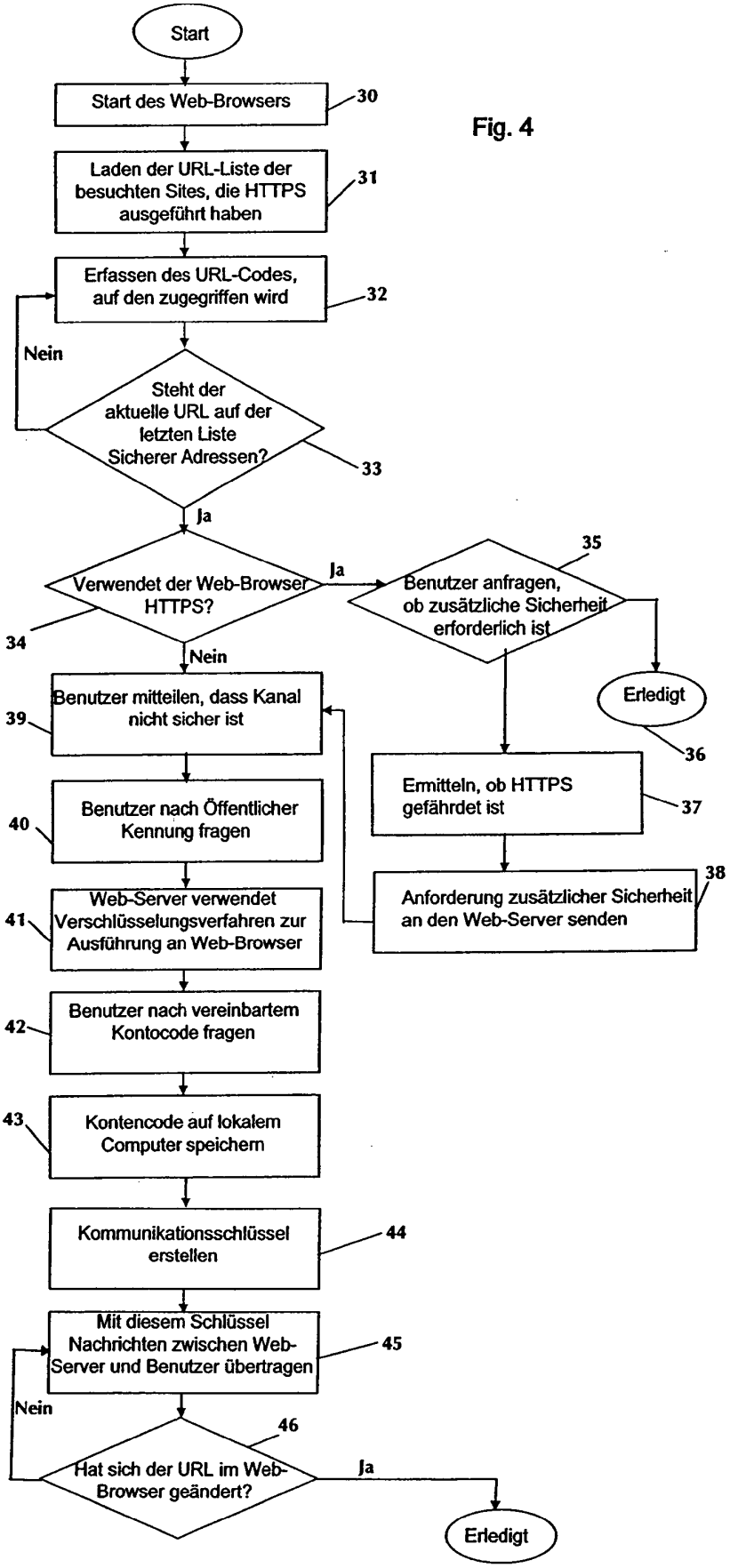

Start
Start des Web-Browsers
30
Laden der URL-Liste der besuchten Sites, die HTTPS ausgeführt haben
31
Erfassen des URL-Codes, auf den zugegriffen wird
32
Nein
Steht der aktuelle URL auf der letzten Liste Sicherer Adressen?
33
Ja
Verwendet der Web-Browser HTTPS?
34
Ja
35
Benutzer anfragen, ob zusätzliche Sicherheit erforderlich ist
Erledigt
36
Nein
Benutzer mitteilen, dass Kanal nicht sicher ist
39
Ermitteln, ob HTTPS gefährdet ist
37
Benutzer nach Öffentlicher Kennung fragen
40
Anforderung zusätzlicher Sicherheit an den Web-Server senden
38
Web-Server verwendet Verschlüsselungsverfahren zur Ausführung an Web-Browser
41
Benutzer nach vereinbartem Kontocode fragen
42
Kontencode auf lokalem Computer speichern
43
Kommunikationsschlüssel erstellen
44
Mit diesem Schlüssel Nachrichten zwischen Web-Server und Benutzer übertragen
45
Nein
Hat sich der URL im Web-Browser geändert?
46
Ja
Erledigt

Fig. 4