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

(10) **DE 60 2004 012 996 T2** 2009.05.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 625 690 B1**
(21) Deutsches Aktenzeichen: **60 2004 012 996.8**
(86) PCT-Aktenzeichen: **PCT/US2004/014379**
(96) Europäisches Aktenzeichen: **04 760 929.2**
(87) PCT-Veröffentlichungs-Nr.: **WO 2004/102338**
(86) PCT-Anmeldetag: **06.05.2004**
(87) Veröffentlichungstag der PCT-Anmeldung: **25.11.2004**
(97) Erstveröffentlichung durch das EPA: **15.02.2006**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.04.2008**
(47) Veröffentlichungstag im Patentblatt: **28.05.2009**

(51) Int Cl.[8]: ***G06F 1/00*** (2006.01)
G06F 17/30 (2006.01)
H04L 29/06 (2006.01)

(30) Unionspriorität:
435322 **09.05.2003** **US**

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR

(73) Patentinhaber:
RSA Security Inc., Bedford, Mass., US

(74) Vertreter:
BOEHMERT & BOEHMERT, 80336 München

(72) Erfinder:
GASPARINI, Louis, San Mateo, CA 94402, US;
GOTLIEB, Charles, San Francisco, CA 94123, US

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUM AUTHENTIFIZIEREN VON BENUTZERN UND WEBSITES**

Beschreibung

[0001] Die vorliegende Erfindung betrifft die Rechnersicherheit und genauer die Rechnersicherheit für das World Wide Web.

Allgemeiner Stand der Technik

[0002] Das Internet und das World Wide Web gestatten Nutzern, mit Software, die an verschiedenen Stellen im Web ausgeführt wird, zu kommunizieren. Es kann jedoch hilfreich sein, einer dieser Einheiten, oder beiden, die Sicherstellung zu gestatten, dass die andere Einheit, mit der diese Einheit kommuniziert, wirklich jene andere Einheit ist.

[0003] Wenn die Website glaubt, dass sie mit einer Einheit kommuniziert, aber tatsächlich mit einer anderen Einheit kommuniziert, kann sie einen Zugang zu heiklen Informationen der Einheit gestatten, mit der sie fälschlicherweise zu kommunizieren glaubt. Sie kann im Namen jener Einheit, mit der sie zu kommunizieren glaubt, die Übertragung von Wertpapieren, den Versand von Produkten oder die Lieferung von Diensten an die andere Einheit verursachen. Zum Beispiel verlieren einige Betreiber von Webseiten beträchtliche Mengen an Geld, indem sie Dieben, die sich der Website fälschlich als registrierter Nutzer identifizieren, Produkte senden oder Bargeld oder andere Wertpapiere übertragen.

[0004] Viele dieser Diebe bringen die Nutzer durch Täuschung dazu, vertrauliche Informationen bereitzustellen, die der Dieb verwenden kann, um sich als registrierter Nutzer zu identifizieren, indem er dem Nutzer gegenüber so auftritt, als ob eine durch den Dieb betriebene Website tatsächlich eine Website wäre, bei der sich der Nutzer registriert hat. Zum Beispiel kann ein Dieb eine Menge an E-Mails aussenden, die den Nutzer mit einem Link zur Website „paypal.com" einladen, sich bei „paypal.com" einzuloggen, wobei er hofft, dass der Empfänger der E-Mail bei der Zahlungswebsite „paypal.com" registriert ist. Der Dieb schreibt jedoch den letzten Buchstaben bei seiner Site groß, so dass sich diese „paypal.com" liest, und hofft, dass das „l" wie der kleingeschriebene letzte Buchstabe „l" in „paypal" aussieht. Die Webseiten, die durch die Website „paypai.com" bereitgestellt werden, werden dann so gestaltet, dass sie wie die Website „paypal.com" aussehen, und wenn sich der Nutzer einzuloggen versucht, werden der Benutzername und das Passwort des Nutzers durch die Website des Diebs erfasst. Der Dieb loggt sich dann unter Verwendung des Benutzernamens und des Passworts des Nutzers, die so empfangen wurden, bei „paypal.com" ein und autorisiert die Übertragung von Geld vom Konto des Nutzers auf ein Konto, das durch den Dieb kontrolliert wird.

[0005] Bei einer anderen Variation des Betrugs stellt der Dieb dem Nutzer einen Link bereit, der ein URL der tatsächlichen Site zu enthalten scheint, aber tatsächlich ein Befehl zum Einloggen bei der Site des Diebs ist. Zum Beispiel kann ein Link, der http:// mit dem Anhang „www.paypal.com/%sdafghdgk%fdsgsdhdsh..." lautet, als echter Link zu „paypal.com" mit einer langen Liste von Parametern, die sich über das Ende des URL-Fensters im Browser des Nutzers erstrecken, erscheinen. Der Nutzer weiß jedoch nicht, dass der obige Link tatsächlich mit „...@paypai.com" endet, was verursacht, dass der Nutzer bei der Website „paypai.com" eingeloggt wird, wobei der Satz von Zeichen links vom Zeichen „@" als Benutzername verwendet wird. Die Website „paypai.com" gestattet jedem derartigen Benutzernamen, sich bei der Website einzuloggen, und geht dann wie oben beschrieben vor, indem sie dem Nutzer eine Nachbildung der Nutzerschnittstelle von „paypal.com" zeigt, die dem Nutzer gestattet, sich bei der Anwendungssoftware an der Website des Diebs einzuloggen (obwohl der falsche Benutzername über den Link bereitgestellt wurde), die dann den Benutzernamen und das Passwort, die so empfangen wurden, verwendet, um sich bei der echten Website „paypal.com" einzuloggen und die Übertragung vorzunehmen.

[0006] Um dieses Problem zu bekämpfen, stellen einige Websites ein Zertifikat bereit, um dem Nutzer zu gestatten, zu verifizieren, dass die Website echt ist, doch sind die Vorgänge zur Durchführung solch einer Authentifizierung komplex, mühsam und den meisten Nutzern unbekannt. Daher sind herkömmliche Verfahren, die verwendet werden könnten, um einem Nutzer zu gestatten, die Website zu authentifizieren, unwirksam, da sie zu schwierig zu verwenden sind. Zum Beispiel lehrt WO 01/63878 A1 das Authentifizieren einer Website auf Basis eines Verifikationsservers und einer einzigartigen seriellen Seitennummer.

[0007] Es kann nicht nur ein unehrlicher Betreiber einer Website einen Nutzer dazu verleiten, zu glauben, dass eine Website echt ist, sondern es kann auch ein unehrlicher Nutzer eine echte Website dazu verleiten, zu glauben, dass der Nutzer echt ist. Wie oben beschrieben, können vertrauliche Informationen von einem Nutzer erfasst werden und dann verwendet werden, um die Website zu veranlassen, zu glauben, dass sie es mit diesem Nutzer zu tun hat. Einige Websites setzen Cookies in den Rechner des Nutzers, und diese Cookies könnten verwendet werden, um zu versuchen, die Möglichkeit zu verifizieren, dass die Person, die sich einzuloggen versucht, tatsächlich jene Person ist. Doch ein Cookie kann durch einen Dieb gefälscht werden, um anzuzeigen, dass es sich beim Rechnersystem des Diebs um das Rechnersystem eines Nutzers handelt, als der sich der Dieb auszugeben versucht.

[0008] Was benötigt wird, sind ein System und ein

Verfahren, die einer Website einen Nutzer sicher authentifizieren können, dem Nutzer eine Website leicht authentifizieren können, ohne dass der Nutzer komplexe Authentifizierungsvorgänge verwenden muss, oder beides.

Kurzdarstellung der Erfindung

[0009] Ein System und ein Verfahren stellen ein verschlüsseltes signiertes Cookie in einem Rechnersystem eines Nutzers bereit, um der Website zu gestatten, den Nutzer zu identifizieren und zu authentifizieren. Zusätzlich oder alternativ wird eine personalisierte Information mit einer Kennung des Nutzers verknüpft, um dem Nutzer zu gestatten, zu erkennen, dass die Website echt ist. Wenn der Nutzer eine Webseite anfordert, wird das Cookie durch die Website aufgerufen und kann die Signatur geprüft werden, um den Nutzer zu authentifizieren. Eine Kennung im Cookie kann verwendet werden, um den Nutzer zu identifizieren und der Website zu gestatten, die personalisierte Information, die der Nutzer erkennen kann, um die Website zu authentifizieren, bereitzustellen. Der Nutzer kann dann eine Site verwenden, die die personalisierte Information bereitstellt, die der Nutzer erwartet. Wenn die personalisierte Information fehlt oder andersartig ist, kann der Nutzer die Bereitstellung von vertraulichen Informationen an diese Website verweigern oder es ablehnen, durch die Website bereitgestellte Informationen zu glauben, wodurch sein Benutzername und Passwort und andere vertrauliche Informationen vor einem Dieb geschützt werden.

Kurze Beschreibung der Zeichnungen

[0010] Fig. 1 ist ein schematisches Blockdiagramm eines herkömmlichen Rechnersystems.

[0011] Fig. 2 ist ein schematisches Blockdiagramm eines Systems, um einem Nutzer zu gestatten, eine Website zu authentifizieren, und der Website zu gestatten, den Nutzer zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung.

[0012] Fig. 3A ist ein Ablaufdiagramm, das ein Verfahren zum Registrieren eines Nutzers, um dem Nutzer zu gestatten, eine Website zu authentifizieren, und der Website zu gestatten, den Nutzer zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht.

[0013] Fig. 3B ist ein Ablaufdiagramm, das ein Verfahren, um einer Website zu gestatten, einen Nutzer zu authentifizieren, und/oder dem Nutzer zu gestatten, die Website zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht.

[0014] Fig. 4 ist ein Ablaufdiagramm, das ein Verfahren, um einen Teil einer Website oder die gesamte Website durch einen Nutzer zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht.

Ausführliche Beschreibung einer bevorzugten Ausführungsform

[0015] Die vorliegende Erfindung kann als Rechnersoftware auf einem herkömmlichen Rechnersystem ausgeführt werden. Unter nun erfolgender Bezugnahme auf Fig. 1 ist ein herkömmliches Rechnersystem **150** zur Ausführung der vorliegenden Erfindung gezeigt. Ein Prozessor **160** ruft Softwarebefehle, die in einer Speichereinheit **162** wie etwa einem Speicher, der ein Direktzugriffsspeicher (RAM) sein kann, gespeichert sind, ab und führt sie aus und kann andere Bestandteile steuern, um die vorliegende Erfindung auszuführen. Die Speichereinheit **162** kann verwendet werden, um Programmbefehle oder Daten oder beides zu speichern. Eine Speichereinheit **164**, wie beispielsweise eine Rechnerfestplatte oder ein anderer nichtflüchtiger Speicher, kann eine Speicherung von Daten oder Programmbefehlen bereitstellen. In einer Ausführungsform stellt die Speichereinheit **164** eine Langzeitspeicherung von Befehlen und Daten bereit, während die Speichereinheit **162** eine Speicherung von Daten oder Befehlen bereitstellt, die möglicherweise nur für eine kürzere Zeit als jene der Speichereinheit **164** benötigt werden. Eine Eingabevorrichtung **166**, wie etwa eine Rechnertastatur oder eine Maus oder beides, gestattet dem Nutzer Eingaben in das System **150**. Eine Ausgabe **168**, wie etwa eine Anzeige oder ein Drucker, gestattet dem System, dem Nutzer des Systems **150** Informationen wie etwa Befehle, Daten oder andere Informationen bereitzustellen. Eine Speichereinheits-Eingabevorrichtung **170**, wie etwa ein herkömmliches Floppy-Disk-Laufwerk oder ein CD-ROM-Laufwerk, nimmt über eine Eingabe **172** Rechnerprogrammprodukte **174**, wie etwa eine herkömmliche Floppy-Disk oder CD-ROM oder ein anderes nichtflüchtiges Speichermedium, das verwendet werden kann, um Rechnerbefehle oder Daten zum System **150** zu transportieren, auf. Auf dem Rechnerprogrammprodukt **174** sind rechnerlesbare Programmcodevorrichtungen **176**, wie etwa magnetische Ladungen im Fall einer Floppy-Disk oder optische Codierungen im Fall einer CD-ROM, codiert, die als Programmbefehle, Daten oder beides codiert sind, um das Rechnersystem **150** dazu einzurichten, wie nachstehend beschrieben zu arbeiten.

[0016] In einer Ausführungsform ist jedes Rechnersystem **150** eine herkömmliche SUN-MICROSYSTEMS ULTRA-10-Workstation, die das von der SUN MICROSYSTEMS, Inc., Mountain View, Kalifornien im Handel erhältliche Betriebssystem SOLARIS ausführt, ein PENTIUM-kompatibles Personalrechnersystem, wie sie von der DELL COMPUTER CORPO-

RATION, Round Rock, Texas, erhältlich sind, das eine Version des von der MICROSOFT Corporation, Redmond, Washington, im Handel erhältlichen Betriebssystems WINDOWS (wie etwa 95, 98, Me, XP, NT oder 2000) ausführt, oder ein Macintosh-Rechnersystem, das das von der APPLE COMPUTER CORPORATION, Cupertino, Kalifornien, im Handel erhältliche Betriebssystem MACOS oder OPENSTEP und den von der NETSCAPE COMMUNICATIONS CORPORATION, Mountain View, Kalifornien, im Handel erhältlichen Browser NETSCAPE oder den von der obigen Firma MICROSOFT im Handel erhältlichen Browser INTERNET EXPLORER ausführt, obwohl andere Systeme verwendet werden können.

[0017] Unter nun erfolgender Bezugnahme auf Fig. 2 ist ein System **200**, um einem Nutzer zu gestatten, eine Website zu authentifizieren, und der Website zu gestatten, den Nutzer zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung gezeigt. Obwohl hierin diese beiden Funktionen beschrieben sind, kann in einer Ausführungsform eine dieser Funktionen ohne die andere verwendet werden: es ist nicht nötig, beide Funktionen nach der vorliegenden Erfindung einzusetzen, obwohl andere Ausführungsformen beide Funktionen einsetzen.

[0018] Das System **200** umfasst einen oder mehrere Server und einen oder mehrere Clients, wobei ein stellvertretender Server **202** und ein stellvertretender Client **260** gezeigt sind, obwohl mehrere Clients gleichzeitig oder zu unterschiedlichen Zeiten auf den Server **202** zugreifen können und mehrere Server gleichzeitig verwendet werden können. Der Server **202** ist mit einem Obersatz von Bestandteilen gezeigt, und es können mehrere Server vorhanden sein, die jeweils den gezeigten Obersatz von Bestandteilen oder eine Teilmenge davon aufweisen können.

[0019] In einer Ausführungsform wird die gesamte Kommunikation in den Server **202** oder daraus hinaus über einen Eingang/Ausgang **208** einer Kommunikationsschnittstelle **210** vorgenommen, die mit einem Netzwerk **254**, wie etwa dem Internet oder einem lokalen Netzwerk oder beiden gekoppelt ist. Die Kommunikationsschnittstelle **210** ist eine herkömmliche Kommunikationsschnittstelle, die Ethernet, TCP/IP oder andere herkömmliche Kommunikationsprotokolle unterstützt.

[0020] Die Kommunikation in den Client **260** und daraus hinaus wird über einen Eingang/Ausgang **258** einer Kommunikationsschnittstelle **262** vorgenommen, die eine herkömmliche Kommunikationsschnittstelle umfasst, welche der Kommunikationsschnittstelle **210** ähnlich oder damit identisch ist, aber auch herkömmliche Schaltungen enthalten kann, um über einen Eingang/Ausgang **256** eine Kopplung an eine herkömmliche Tastatur/einen herkömmlichen Bildschirmeine herkömmliche Maus (nicht gezeigt) oder eine andere ähnliche herkömmliche Eingabe/Ausgabevorrichtung vorzunehmen. Die Kommunikationsschnittstelle **262** kann über ein Modem, das mit einem Eingang/Ausgang **258** gekoppelt ist, der ebenfalls ein Teil der Kommunikationsschnittstelle **262** ist, mit dem Netzwerk **254** gekoppelt sein.

[0021] Wie nachstehend ausführlicher beschrieben ist, wird in einer Ausführungsform ein Registrierungsprozess durchgeführt, um eine personalisierte Information für jeden Nutzer zu identifizieren, um dem Nutzer zu gestatten, die Website wahrnehmbar zu authentifizieren. Eine derartige wahrnehmbare Authentifizierung kann alles beliebige beinhalten, das zur Feststellung durch den Nutzer fähig ist, wie etwa das Aussehen einer oder mehrerer Webseiten, ein oder mehrere Geräusche, die damit auftretend bereitgestellt werden, ein Geruch, eine Tasteindruck oder ein Geschmack. Zum Beispiel kann auf der anfänglichen Einlogseite der Website und optional auf nachfolgenden Seiten ein Foto des Nutzers erscheinen, um dem Nutzer zu zeigen, dass die Seite echt ist. Anstelle des Fotos, oder zusätzlich dazu, kann eine bestimmte Textpassage verwendet werden. Zusätzlich zu jedem der genannten Beispiele, oder stattdessen, kann ein dem Nutzer bekanntes Geräusch verwendet werden.

[0022] Wie nun beschrieben werden wird, verbindet der Registrierungsprozess eine Kennung des Nutzers mit der personalisierten Information, die dem Nutzer bereitgestellt wird, um dem Nutzer zu gestatten, die Website zu authentifizieren. In einer Ausführungsform stellt der Nutzer die personalisierte Information bereit oder wählt diese aus, während in einer anderen Ausführungsform ein Systemadministrator diese Funktion durchführt und dann den Nutzer von der personalisierten Information in Kenntnis setzt.

[0023] In einer Ausführungsform verwendet der Nutzer einen herkömmlichen Browser **264**, die Kommunikationsschnittstelle **262** und das Netzwerk **254**, um sich über eine über die Kommunikationsschnittstelle **210** empfangene Anforderung nach einer Webseite, die der Webanwendungs-Einheit **240** auf Basis der Portnummer der Anforderung bereitgestellt wird, in den Server **202** einzuloggen. Obwohl der Browser **264** wie hierin beschrieben verwendet wird, können andere Ausführungsformen eine Betriebssystemsoftware, ein Servlet oder eine andere Anwendungssoftware verwenden.

[0024] Die Webanwendungs-Einheit **240** lenkt den Browser des Nutzers zu einem SSL-Port am Server **202** (oder einem anderen Server, der dem hierin beschriebenen Server **202** ähnlich oder damit identisch ist) um, und der Browser **264** des Nutzers sendet die Anforderung neuerlich über eine SSL-Verbindung,

die die Kommunikationsschnittstelle **210** einer Verschlüsselte-Kommunikation-Verwaltungseinheit **212** bereitstellt. Die Verschlüsselte-Kommunikation-Verwaltungseinheit **212** verwendet herkömmliche SSL-Verarbeitungstechniken, um die Verbindung herzustellen, die Anforderung zu empfangen und die Anforderung zu entschlüsseln, und stellt die entschlüsselte Anforderung der Webanwendungs-Einheit **240** bereit.

[0025] Die Webanwendungs-Einheit **240** versucht, ein Cookie zu lesen, das in einer Cookiespeichereinheit **266** gespeichert worden sein kann und, falls es so gespeichert worden ist, dem Server **202** durch den Browser **264** als Teil der Verbindung bereitgestellt wurde. In einer Ausführungsform erzeugt die Webanwendungs-Einheit **240** bei Nichtvorhandensein des Cookies (oder in einer anderen Ausführungsform in allen Fällen) eine Webseite (die dem Nutzer auch gestatten kann, sich wie nachstehend beschrieben einzuloggen), die einen Link zu einer durch eine Registrierungseinheit **222** bereitgestellten Registrierungsseite beinhaltet. Wenn der Nutzer den Link anklickt, wird der Browser **264** des Nutzers die Registrierungsseite anfordern, die die oben beschriebene SSL-Verbindung oder eine andere SSL-Verbindung verwenden kann. Die Kommunikationsschnittstelle **210** wird die Anforderung empfangen und sie der Registrierungseinheit **222** über eine SSL-Verbindung über die Verschlüsselte-Kommunikation-Verwaltungseinheit **212** bereitstellen, und die Registrierungseinheit **222** stellt die Seite über die Kommunikationsschnittstelle **210** und die Verschlüsselte-Kommunikation-Verwaltungseinheit **212**, die die SSL-Verbindung verwendet, bereit.

[0026] Der Nutzer kann ein ausreichendes Kennzeichen bereitstellen, um anzuzeigen, dass der Nutzer ist, wer der Nutzer zu sein behauptet. Dieser Prozess wird durch die Registrierungseinheit **222** erzwungen, obwohl er auf eine breite Vielfalt von Weisen durchgeführt werden kann.

[0027] In einer Ausführungsform verlangt die durch die Registrierungseinheit **222** bereitgestellte Webseite zur Registrierung den Benutzernamen und/oder das Passwort einer Person, die die Identität der Partei verifiziert hat, welche die Registrierungseinheit **222** zuvor in einer Datenbank **224** gespeichert hat, so dass der Benutzername und/oder das Passwort, die bereitgestellt werden, durch die Registrierungseinheit **222** mit einem Satz von autorisierten Benutzernamen und Passwörtern verglichen werden können, um zu bestimmen, ob der Nutzer ein ausreichendes Kennzeichen seiner Identität bereitgestellt hat. In einer anderen Ausführungsform fragt die Registrierungseinheit **222** den Nutzer nach einem anderen Satz einer oder mehrerer Kennungen, die dem Nutzer durch bandexterne Mittel wie etwa die Post, ein Fax oder das Telefon oder durch eine andere Webverbindung oder eine E-Mail-Nachricht bereitgestellt wurden und die durch die Registrierungseinheit **222** früher erzeugt und dem Nutzer bereitgestellt wurden.

[0028] Abhängig von den Sicherheitsanforderungen der Website kann der Nutzer ein derartiges ausreichendes Kennzeichen seiner Identität ohne derartige andere systembereitgestellte Informationen bereitstellen. Diese können eine Nutzerkennung und ein Passwort sein, können aber auch der Mädchenname einer Mutter oder andere Informationen sein, die früher vom Nutzer oder einer anderen Quelle eingeholt wurden und in der Datenbank **224** gespeichert wurden. Es kann eine Frage-und-Antwort-Vorkehrung verwendet werden, wobei eine oder mehrere Fragen zufällig durch die Registrierungseinheit **222** ausgewählt werden und dem Nutzer gestellt werden, und die Registrierungseinheit **222** die Antworten empfangt und die Antworten auf die Fragen (z. B. den Namen eines Haustiers) mit Aufzeichnungen in der Datenbank **224** vergleicht, die mit einem Benutzernamen (und optional einem Passwort) entsprechen, der der Registrierungseinheit **222** durch den Nutzer ebenfalls über das gleiche Webseitenformular oder ein durch die Registrierungseinheit bereitgestelltes anderes Webseitenformular bereitgestellt wird. In einer anderen Ausführungsform können der Benutzername oder der Benutzername und das Passwort, die der Registrierungseinheit **222** durch den Nutzer über ein Webseitenformular bereitgestellt werden, das die Einheit als Reaktion auf die Anforderung erzeugt, ein ausreichendes Identifikationskennzeichen sein. In noch einer anderen Ausführungsform braucht sich der Nutzer nicht selbst der Registrierungseinheit **222** gegenüber zu authentifizieren, und in einer derartigen Ausführungsform ist der Umstand, dass die Partei zu einer bestimmten Zeit, von einer bestimmten IP-Adresse oder anderweitig mit der Website verbunden ist, ein ausreichendes Identifikationskennzeichen.

[0029] Sobald die Registrierungseinheit **222** vom Nutzer ein ausreichendes Identifikationskennzeichen empfangen hat, erzeugt sie eine Kennung oder verwendet eine bestehende Kennung für den Nutzer (die die gleiche wie der Benutzername oder eine andere Kennung, die durch den Nutzer geliefert wurde, oder eine Kennung sein kann, die der Aufzeichnung in der Datenbank **224**, die andere Informationen für den Nutzer hält, entspricht) und speichert die Kennung in einem Eintrag für den Nutzer in der Datenbank **224**, falls die Kennung nicht bereits in irgendeinem derartigen Eintrag, der bereits für diesen Nutzer bestehen kann, gespeichert ist.

Der Nutzer stellt eine personalisierte Information bereit

[0030] Nachdem der Nutzer ein ausreichendes Kennzeichen der Identität des Nutzers bereitgestellt

hat, veranlasst die Registrierungseinheit **222** den Nutzer, eine personalisierte Information aus einer vordefinierten Liste auszuwählen oder bereitzustellen, die dem Nutzer zum Teil oder zur Gänze gezeigt werden kann, wenn vom Nutzer verlangt wird, der Website vertrauliche oder andere Informationen bereitzustellen. Wie oben erwähnt, kann in einer anderen Ausführungsform ein Systemadministrator die personalisierte Information für einen Nutzer auswählen oder bereitstellen.

[0031] Die personalisierte Information kann alles beliebige sein, das der Nutzer verwenden kann, um zu erkennen, dass die Website echt ist. Sie kann jede beliebige Anzahl aus dem Folgenden sein: ein Foto, eine Grafik, eine Farbe, ein Layout, eine Nachricht, ein Ton, ein Geruch oder alles beliebige, das durch eine Berührung gefühlt werden kann. Die personalisierte Information kann aus einer Liste gewählt werden oder kann eine Originalinformation sein, die durch den Nutzer bereitgestellt wird, der sie verwenden wird, um die Authentizität der Website zu identifizieren, wie etwa ein digitales Foto seiner selbst. Die personalisierte Information muss nicht statisch sein, sie kann eine Formel wie etwa „heute ist @Datum", wobei „@Datum" durch das Datum jenes Tages ersetzt ist, oder „nur(@5. Mai-heute)Tage bis zu Ihrem Geburtstag", wobei „(@5. Mai-heute)" durch die Anzahl der Tage bis zum kommenden 5. Mai ersetzt ist, sein.

[0032] Die Registrierungseinheit **222** stellt eine Webseite bereit, um dem Nutzer zu gestatten, jede beliebige Anzahl eines jeden der obigen Punkte zu wählen oder bereitzustellen, und speichert dann die Punkte oder Angaben der Punkte in der Datenbankaufzeichnung für den Nutzer in der Datenbank **224**. In noch einer anderen Ausführungsform erzeugt die Registrierungseinheit **222** eine derartige personalisierte Information oder wählt diese (d. h., zufällig) und stellt sie dem Nutzer bereit und speichert sie in der Datenbankaufzeichnung. Die personalisierte Information kann, wie oben beschrieben, über die Webseite oder bandextern bereitgestellt werden.

[0033] In einer Ausführungsform stellt die Registrierungseinheit **222** die personalisierte Information über die Verschlüsselte-Kommunikation-Verwaltungseinheit **212** bereit oder fragt sie über diese Einheit ab und empfängt sie über diese Einheit, welche einen sicheren Kommunikationskanal, wie etwa SSL-verschlüsselte Kommunikationen, einleitet und verwendet, um die personalisierte Information bereitzustellen oder abzufragen und zu empfangen, um zu verhindern, dass Andere die personalisierte Information abfangen.

Ein Cookie wird verschlüsselt, signiert und gespeichert

[0034] Die Registrierungseinheit **224** leitet auch die Speicherung eines signierten verschlüsselten Cookies im Rechnersystem des Nutzers ein. Diese Speicherung kann zu jeder beliebigen Zeit nach der oben beschriebenen Bereitstellung eines ausreichenden Kennzeichens der Identität des Nutzes durch den Nutzer durchgeführt werden und kann entweder vor, nach oder anstelle der oben beschriebenen Identifikation einer personalisierten Information durchgeführt werden.

[0035] Um das Cookie zu erzeugen und zu speichern, stellt die Registrierungseinheit **224** einer Cookie-Erzeugungseinheit **230** die Kennung des Nutzers bereit, die, wie oben beschrieben, in dem Eintrag des Nutzers in der Datenbank **224** gespeichert ist. Die Cookie-Erzeugungseinheit **230** nimmt die Nutzerkennung in das Cookie auf und kann dem Cookie andere Zustandsinformationen hinzufügen und stellt die Kennung und die anderen Informationen einer Cookie-Signatureinheit **232** bereit, die das Cookie unter Verwendung herkömmlicher kryptographischer Techniken, wie etwa durch Hashen der Kennung und optional der anderen Informationen unter Verwendung eines geheimen Hash-Schlüssels, um ein hierin als Cookie-Signatur bezeichnetes Hash-Ergebnis zu erzeugen, signiert. Die Cookie-Signatureinheit **232** stellt die Cookie-Signatur, die Kennung und optional die anderen Informationen, die gesammelt als das Cookie bezeichnet werden, einer Cookie-Verschlüsselungseinheit **234** bereit, die das Cookie unter Verwendung herkömmlicher Verschlüsselungstechniken, wie etwa unter Verwendung des öffentlichen Schussels eines Paars aus einem öffentlichen Schlüssel und einem privaten Schlüssel oder unter Verwendung eines symmetrischen Schlüssels, verschlüsselt. Die Cookie-Verschlüsselungseinheit **234** veranlasst dann den Browser **264**, das verschlüsselte Cookie über die Verschlüsselte-Kommunikation-Verwaltungseinheit **212**, die Kommunikationsschnittstelle **210**, das Netzwerk **254** und die Kommunikationsschnittstelle **262**, optional unter Verwendung einer SSL-Verbindung, wie etwa die Verbindung, die wie oben beschrieben für die Registrierung verwendet wird, in der Cookie-Speichereinheit **266** im Clientrechnersystem **260** des Clients zu speichern. Die Cookie-Speichereinheit **266** kann ein herkömmlicher Speicher oder eine Plattenspeichereinrichtung sein und kann ein Teil davon sein, der zur Speicherung von Cookies verwendet wird, und kann ein Teil des Clientrechnersystems **260** sein oder sich in einer entfernbaren Vorrichtung, wie etwa einer Smartcard, einem USB-Speicher-Token (einer tragbaren Speichervorrichtung, die durch einen USB-Anschluss mit einem Personalrechner gekoppelt wird, wie etwa der von Dell Computer Systems, Round Rock, Texas, im Handel erhältliche USB-Memo-

ry-Key) oder dergleichen befinden. Obwohl, wie hierin beschrieben, ein Cookie verwendet wird, können andere Ausführungsformen Arten von verschlüsselten Dateien, Zertifikate oder andere ähnliche Datenstrukturen einsetzen.

[0036] In einer Ausführungsform braucht das Clientrechnersystem **260** des Nutzers nicht für die anfängliche Registrierung verwendet zu werden. Stattdessen kann der Registrierungsprozess in zwei Teilen durchgeführt werden: Der erste Teil gestattet dem Nutzer, die Wahl personalisierter Information, wie oben beschrieben, von einem bestimmten Satz von Browser, die bekannte IP-Adressen aufweisen oder unter Verwendung eines Systemadministratornutzers, einer Kennung und eines Passworts authentifiziert werden. Der zweite Teil gestattet dem Nutzer, sich wie oben beschrieben unter Verwendung des Kennzeichens der Identität des Nutzers von seinem eigenen Browser einzuloggen, zu welcher Zeit das verschlüsselte Cookie in das Clientrechnersystem **260** des Nutzers gesetzt wird.

Verifizieren der Identität der Webseite und/oder des Nutzers

[0037] Im Anschluss an den oben beschriebenen Empfang des Cookies wird der Nutzer, wenn der Nutzer eine Webseite von der Website anfordert, seinen Webbrowser **264** verwenden, um die Anforderung zum Server **202** zu senden. Der Browser **264** sendet die Anforderung über die Kommunikationsschnittstellen **262** und **210** und das Netzwerk **254** zum Server **202**. Die Kommunikationsschnittstelle **210** gibt die Anforderung zur Webanwendungs-Einheit **240** weiter, bei der es sich um ein wie hierin beschrieben modifiziertes herkömmliches Webanwendungs-Programm handelt. Die Webanwendungs-Einheit **240** kann den Nutzer authentifizieren, die personalisierte Information bereitstellen, um dem Nutzer zu gestatten, die Website zu authentifizieren, oder beides, wie nun beschrieben werden wird.

[0038] Um den Nutzer zu authentifizieren, liest die Webanwendungs-Einheit **240** das verschlüsselte Cookie, das durch den Browser **264** bereitgestellt wird, aus der Cookie-Speichereinheit **266**, wobei dieses Cookie wie hierin beschrieben in die Cookie-Speichereinheit **266** gesetzt wird. Die Webanwendungs-Einheit **240** gibt das verschlüsselte Cookie zur Nutzer-Authentifizierungs-Einheit **242** weiter, die das verschlüsselte Cookie entschlüsselt und dann die Signatur vom Rest des Cookies trennt. Die Nutzer-Authentifizierungs-Einheit **242** verifiziert, dass die Signatur dem Rest des Cookies entspricht (z. B. durch Rehashing des Rests des Cookies unter Verwendung des gleichen Hash-Algorithmus und Hash-Schlüssels, die zum Erzeugen der Signatur verwendet wurden, und Vergleichen des Hash-Ergebnisses mit der Signatur), und stellt entweder der Webanwendungs-Einheit **240** die Kennung des Nutzers oder andere Informationen, die im Cookie gespeichert sein können, bereit, wenn die Nutzer-Authentifizierungs-Einheit **242** den Nutzer über die Signatur authentifiziert (z. B. das Hash-Ergebnis, das sie erzeugt, mit der Signatur übereinstimmt), oder zeigt an, dass das Cookie nicht gültig ist (z. B. wenn das Hash-Ergebnis, das die Nutzer-Authentifizierungs-Einheit **242** erzeugt, nicht mit der Signatur übereinstimmt).

[0039] Wenn die Nutzer-Authentifizierungs-Einheit **242** angibt, dass das Cookie nicht gültig ist, kann die Webanwendungs-Einheit **240** den Zugang zu einem Teil oder der gesamten Website verweigern. Andernfalls empfangt die Webanwendungs-Einheit **240** die Nutzerkennung und verwendet die Nutzerkennung, um die Webanwendungs-Einheit **240** zu betreiben und/oder dem Nutzer eine wie hierin beschrieben gewählte personalisierte Information bereitzustellen.

[0040] Die personalisierte Information kann mit jeder Webseite, die durch die Webanwendungs-Einheit **240** bereitgestellt wird, mit Webseiten, die angezeigt werden, um dem Nutzer vertrauliche Informationen bereitzustellen, mit Webseiten, die verwendet werden, um jedwede Informationen vom Nutzer anzufordern, oder mit Webseiten, die verwendet werden, um vertrauliche Informationen vom Nutzer anzufordern, oder jeder beliebigen Kombination einiger oder aller dieser Beispiele bereitgestellt werden. Vertrauliche Informationen können Informationen, die verwendet werden können, um Zugang zu finanziellen oder anderen Mitteln des Betreibers der Website oder des Nutzers zu erlangen, oder andere Informationen, von denen ein Nutzer nicht wünscht, dass andere darüber Bescheid wissen, beinhalten.

[0041] Die personalisierte Information kann als Teil von oben beschriebenen Webseiten bereitgestellt werden, oder sie kann getrennt bereitgestellt werden. Um die personalisierte Information mit jeder beliebigen der oben beschriebenen Webseiten bereitzustellen, stellt die Webanwendungs-Einheit **240** einer Bereitstellungs-Einheit für personalisierte Information **244** die wie oben beschrieben empfangene Nutzerkennung und die Inhalte einer Webseite, bei der die personalisierte Information weggelassen ist, optional mit einer oder mehreren Angaben in der Webseite, die beschreiben, wie und wo die personalisierte Information in die Webseite einzusetzen ist, zusammen mit der IP-Adresse des Nutzers und anderen Informationen, die verwendet werden können, um die Webseite zu adressieren, bereit.

[0042] Die Bereitstellungs-Einheit für personalisierte Information **244** ruft die personalisierte Information, die in dem Eintrag, welcher der Nutzerkennung entspricht, gespeichert ist, aus der Datenbank **224** ab und stellt die personalisierte Information bereit, in-

dem sie sie zum Beispiel gemäß Anweisungen, die mit der Webseite oder als Teil davon empfangen werden, der Webseite, die sie von der Webanwendungs-Einheit **240** empfängt, hinzufügt, oder indem sie sie an einer bestimmten Stelle in der Webseite bereitstellt, und stellt dem Nutzer die personalisierte Information mit jeder Webseite, die sie empfängt, unter Verwendung der IP-Adresse des Nutzers, die sie empfängt, bereit.

[0043] In einer Ausführungsform kann die personalisierte Information durch die Bereitstellungs-Einheit für personalisierte Information **244** bandextern bereitgestellt werden, etwa indem das Mobiltelefon des Nutzers angerufen wird und dem Nutzer mitgeteilt wird, dass die Webseite echt ist, indem eine Aufzeichnung der Stimme des Nutzers, ein Lieblingslied, eine voraufgezeichnete Nachricht oder anderes abgespielt wird. Die bandexterne personalisierte Information kann über einen Ausgang **243** bereitgestellt werden, der mit einer herkömmlichen Telefonleitung gekoppelt sein kann, wobei die Bereitstellungs-Einheit für personalisierte Information **244** eine geeignete Schnittstelle enthält.

[0044] Wenn der Nutzer die personalisierte Information etwa über den Browser **264** und einen mit dem Eingang/Ausgang **256** gekoppelten Bildschirm oder bandextern empfängt, kann der Nutzer sie verwenden, um die Website zu authentifizieren, und das Bereitstellen von Informationen oder das Verwenden der Website verweigern, wenn die Personalisierung fehlt oder sich von der personalisierten Information, die der Nutzer wie oben beschrieben gewählt oder bereitgestellt hat, unterscheidet. Wenn die personalisierte Information das ist, was wie hierin beschrieben registriert wurde, kann der Nutzer vertrauliche Informationen über Webseiten, die von der Webanwendungs-Einheit **240** bereitgestellt werden, bereitstellen, davon empfangenen Informationen glauben oder beides.

[0045] Obwohl die personalisierte Information hierin so beschrieben ist, als ob sie für jeden Nutzer einen einzelnen Fall aufweisen würde, können für jeden von einigen oder allen Nutzern unterschiedliche Fälle von personalisierten Informationen gespeichert sein, wobei jeder Fall von personalisierter Information eine unterschiedliche Bedeutung aufweist; z. B. kann ein Fall bedeuten, dass es für den Nutzer in Ordnung ist, sichere Informationen bereitzustellen, und kann ein anderer Fall von personalisierter Information für den gleichen Nutzer bedeuten, dass Informationen auf der Seite als von einer echten Quelle bereitgestellt bestätigt sind. Die Verknüpfung jedes Falls von personalisierter Information mit der Kennung des Nutzers kann, zusammen mit einer Kennung des Falls, wie hierin beschrieben durchgeführt werden, und jeder Fall von personalisierter Information für einen Nutzer kann von den anderen Fällen für diesen Nutzer wahrnehmbar unterschiedlich sein. Die Webanwendungs-Einheit **240** stellt dann der Bereitstellungs-Einheit für personalisierte Information **244** die Kennung des Nutzers und eine Kennung des Falls von personalisierter Information, die bereitgestellt werden sollte, bereit, und die Bereitstellungs-Einheit von personalisierter Information **244** verwendet die Kennung des Nutzers und die Kennung des Falls, um den richtigen Fall von personalisierter Information auf die gleiche Weise, wie oben für den einzelnen Fall von personalisierter Information für jeden Nutzer beschrieben wurde, abzurufen und dem Nutzer bereitzustellen.

Die Datenbank kann zentralisiert sein

[0046] In einer Ausführungsform befindet sich die Datenbank **224** nicht im Server, sondern ist statt dessen durch eine Datenbank **224A** ersetzt, die über das Netzwerk **254** für mehr als einen Server **202** zugänglich ist und im Übrigen wie die Datenbank **224** tätig ist. Jeder derartige mehr als eine Server kann die gleiche Website wie der Server **202** oder eine andere Website bedienen. In einer derartigen Ausführungsform gibt es mehr als einen Server **202**, und entweder registriert jeder Server, wie oben beschrieben, Nutzer und stellt eine personalisierte Information bereit, verwendet jedoch die zentrale Datenbank **224A** anstelle der Datenbank **224**, oder es registriert nur ein Teil der Server **202** Nutzer, während die anderen Server von der personalisierten Information, die von den Nutzern identifiziert wird oder einem derartigen Registrierungsserver bereitgestellt wird oder die durch einen derartigen Registrierungsserver, wie er obenstehend beschrieben ist, bereitgestellt wird, Gebrauch machen.

[0047] In einer Ausführungsform verwendet jeder Server **202** eine Nummer, die unter den verschiedenen Server für den gleichen Nutzer einzigartig ist, wie etwa eine Website-Nummer oder eine Servernummer, die einer Nutzerkennung, wie etwa einer Sozialversicherungsnummer des Nutzers, angefügt ist, um auf einen Eintrag eines Nutzers in der Datenbank **224A** zuzugreifen. In einer derartigen Ausführungsform kann anstelle der Bereitstellungs-Einheit für personalisierte Information **244** eine Bereitstellungs-Einheit für personalisierte Information **244A**, die für mehrere Server **202** zugänglich ist, verwendet werden, so dass die Server **202** über keinen Zugriff auf die personalisierte Information des Nutzers verfügen. Die Bereitstellungs-Einheit für personalisierte Information **244A** arbeitet auf die gleiche Weise wie die Bereitstellungs-Einheit für personalisierte Information **244**, um dem Nutzer die personalisierte Information mit der Webseite zu senden.

[0048] In einer Ausführungsform verwenden entweder die Datenbank **224A** oder die Bereitstellungs-Einheit für personalisierte Information **244A**

und die Webanwendungseinheit **240** oder die Bereitstellungs-Einheit für personalisierte Information **244** herkömmliche Authentifizierungstechniken, um Anforderungen einer personalisierten Information oder Anforderungen zum Senden einer Webseite mit einer personalisierten Information zu authentifizieren. Diese Authentifizierungstechniken können Passwörter, digitale Zertifikate oder andere herkömmliche Techniken beinhalten. Derartige Anforderungen können über die Verschlüsselte-Kommunikation-Verwaltungseinheit **212** gesendet werden, so dass herkömmliche SSL-Verbindungen verwendet werden können, um die Sicherheit zu verbessern.

[0049] Unter nun erfolgender Bezugnahme auf Fig. 3A ist ein Ablaufdiagramm gezeigt, das ein Verfahren, um einen Nutzer zu registrieren, um dem Nutzer zu gestatten, eine Website zu authentifizieren, der Website zu gestatten, den Nutzer zu authentifizieren, oder beides, nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht.

[0050] Ein Kennzeichen der Identität eines Nutzers kann wie oben beschrieben erzeugt und bereitgestellt werden **310**. Das in Schritt **310** bereitgestellte Kennzeichen kann in einer Ausführungsform wie oben beschrieben über das Internet oder bandextern (z. B. nicht über das Internet) bereitgestellt werden, und in einer anderen Ausführungsform kann auf Schritt **310** verzichtet werden. Optional werden sichere Kommunikationen mit dem Nutzer eingerichtet **312**. Es wird ein ausreichendes Kennzeichen der Identität des Nutzers angefordert und ein Kennzeichen der Identität des Nutzers empfangen **314**. Wenn das Kennzeichen nicht ausreichend ist **316**, wird der Zugriff auf einen Teil oder den gesamten Rest der Schritte von Fig. 3A verweigert **318** und das Verfahren mit Schritt **314** fortgesetzt, während das Verfahren andernfalls **316** mit Schritt **320** fortsetzt.

[0051] Bei Schritt **320** wird der Nutzer aufgefordert, wie oben beschrieben eine personalisierte Information zu wählen oder bereitzustellen, und die personalisierte Information wird empfangen. Schritt **320** kann über einen sicheren Kommunikationskanal, wie etwa die SSL-verschlüsselte Internet-Verbindung, die in Schritt **312** hergestellt wurde, durchgeführt werden. Die personalisierte Information kann einen durch den Nutzer bereitgestellten Inhalt oder eine Angabe eines oder mehrerer Elemente eines durch den Server bereitgestellten Inhalts beinhalten, der mit einer Kennung des Nutzers verknüpft werden wird. Die personalisierte Information wird mit einer Kennung des Nutzers, die durch den Nutzer geliefert werden kann, aus dem in Schritt **314** empfangenen Kennzeichen nachgeschlagen werden kann oder als Teil von Schritt **322** erzeugt werden kann, gespeichert **322**.

[0052] Unter Verwendung der Nutzerkennung wird, wie oben beschrieben, ein Cookie erzeugt **324** und das Cookie signiert **326**, verschlüsselt **328** und im System des Nutzers gespeichert **330**, und das Verfahren setzt mit Schritt **310** fort.

[0053] Unter nun erfolgender Bezugnahme auf Fig. 3B ist ein Ablaufdiagramm gezeigt, das ein Verfahren, um einer Website zu gestatten, einen Nutzer zu authentifizieren und/oder dem Nutzer zu gestatten, die Website zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht. Die Schritte von Fig. 3B können nach einigen oder allen Schritten von Fig. 3A durchgeführt werden. Eine Anforderung einer Webseite wird empfangen **340** und ein verschlüsseltes Cookie aus der Vorrichtung, von der die Anforderung empfangen wurde, gelesen **342**, und das Cookie wird entschlüsselt. Eine Signatur im entschlüsselten Cookie wird, wie oben beschrieben, geprüft **344**, und wenn die Signatur am Cookie anzeigt, dass das Cookie nicht echt ist **346**, kann der Zugriff auf die angeforderte Webseite verweigert werden **348** und setzt das Verfahren mit Schritt **340** fort, während das Verfahren andernfalls **346** mit Schritt **350** fortsetzt.

[0054] Bei Schritt **350** kann, wenn die Anforderung eine Anforderung einer Webseite ist, die keine vertraulichen Informationen verlangen wird oder keine Informationen bereitstellen wird, für die der Nutzer ein Kennzeichen der Authentifizierung wünschen kann, die angeforderte Webseite bereitgestellt werden **352**, und das Verfahren setzt mit Schritt **340** fort, während das Verfahren andernfalls **350** mit Schritt **354** fortsetzt. In einer anderen Ausführungsform, die durch die gestrichelte Linie in der Figur gezeigt ist, wird die Prüfung von Schritt **350** nicht durchgeführt, und Schritt **354** folgt bedingungslos dem „OK"-Zweig von Schritt **350**.

[0055] Bei Schritt **354** wird eine Nutzerkennung, die im in Schritt **342** abgerufenen Cookie gespeichert ist, wie oben beschrieben verwendet, um eine personalisierte Information, die mit dieser Nutzerkennung verknüpft ist, abzurufen, und kann die personalisierte Information optional in die angeforderte Webseite aufgenommen werden **356** und werden die Webseite und die personalisierte Information bereitgestellt, entweder über eine sichere Verbindung, wenn die personalisierte Information über die gleiche Verbindung wie die Webseite bereitgestellt wird, oder die personalisierte Information kann wie oben beschrieben bandextern bereitgestellt werden **358**.

[0056] Unter nun erfolgender Bezugnahme auf Fig. 4 ist ein Verfahren, um einen Teil einer Website oder die gesamte Website durch einen Nutzer zu authentifizieren, nach einer Ausführungsform der vorliegenden Erfindung gezeigt. Optional wird, wie oben beschrieben, ein ausreichendes Kennzeichen der Identität empfangen (z. B. bandextern) und bereitgestellt **410**. Die personalisierte Information wird, wie

oben beschrieben, identifiziert, wie etwa bereitgestellt, gewählt oder empfangen **412**. Ein verschlüsseltes signiertes Cookie kann, wie oben beschrieben, empfangen und gespeichert werden **414**. Eine Anforderung einer Webseite wird bereitgestellt, und optional wird das verschlüsselte signierte Cookie bereitgestellt **416**. Die Webseite und optional eine bestimmte personalisierte Information werden empfangen, **418** und die personalisierte Information wird mit dem verglichen **420**, was in Schritt **412** bereitgestellt oder gewählt wurde. Wenn die empfangene personalisierte Information dem entspricht **422**, was in Schritt **412** identifiziert wurde (z. B. da sie übereinstimmt), kann die Information empfangen und geglaubt oder bereitgestellt werden **426**, und andernfalls kann es der Nutzer ablehnen, die empfangene Information zu empfangen oder zu glauben, oder es ablehnen, die verlangte Information bereitzustellen **426**.

Patentansprüche

1. Verfahren zur Bereitstellung einer Webseite, das folgende Schritte umfasst:
Verknüpfen von personalisierter Information mit einer Nutzerkennung zumindest als Teil eines Registrierungsverfahrens, das zumindest teilweise zur Festlegung personalisierter Information für einen Nutzer durchgeführt wird, um dem Nutzer die wahrnehmbare Authentifizierung wenigstens der Webseite zu ermöglichen;
Bereitstellen der Nutzerkennung in einem Cookie;
Verschlüsseln des Cookies;
Speichern des Cookies auf einem vom Nutzer betriebenen Rechnersystem;
Auslesen des gespeicherten Cookies in Reaktion auf eine Anforderung der Webseite;
Bereitstellen der angeforderten Webseite;
Bereitstellen der personalisierten Information in Reaktion auf den ausgelesenen Cookie über:
a) eine sichere Verbindung und/oder;
b) einen Verbindungskanal, der sich von dem zur Bereitstellung der Webseite benutzten Kanal unterscheidet; und
Authentifizieren der Webseite durch Vergleich der personalisierten Information mit zuvor bereitgestellter Information.

2. Verfahren nach Anspruch 1, das zusätzlich folgende Verfahrensschritte umfasst: Hinzufügen einer Signatur des Cookies zum Cookie vor dem Speicherschritt; und Verifizieren der Signatur des ausgelesenen Cookies.

3. Verfahren nach Anspruch 1 oder 2, wobei die personalisierte Information als Teil der Webseite bereitgestellt wird.

4. Verfahren nach Anspruch 1 oder 2, wobei die personalisierte Information im Wesentlichen gleichzeitig mit der Webseite, aber davon getrennt, bereitgestellt wird.

5. Verfahren nach einem der vorangehenden Ansprüche, wobei der Schritt des Bereitstellens der personalisierten Information das Bereitstellen der Nutzerkennung von dem ausgelesenen Cookie über ein Netzwerk zu einer Datenbank umfasst.

6. Verfahren nach Anspruch 1, das zusätzlich den Schritt umfasst, ein Kennzeichen einer Authentifizierung des Nutzers zu empfangen, wobei der Schritt des Verknüpfen in Reaktion auf den Schritt des Empfangens des Kennzeichens erfolgt.

7. Verfahren nach Anspruch 6, wobei das Kennzeichen ein System-Administratorpasswort umfasst.

8. Verfahren zur Authentifizierung zumindest eines Teils einer Webseite mit folgenden Schritten:
elektronisches Bereitstellen einer Anforderung nach wenigstens einer Webseite und eines verschlüsselten Cookies an einen die Webseite umfassenden Netzserver;
elektronisches Empfangen einer Webseite und von personalisierter Information, die zuvor zumindest als Teil eines Registrierungsverfahrens empfangen wurde, das zumindest teilweise zur Festlegung von personalisierter Information für einen Nutzer durchgeführt wurde, um dem Nutzer die wahrnehmbare Authentifizierung zumindest der Webseite zu ermöglichen; und
Authentifizieren zumindest des Teils der Webseite als Reaktion auf die empfangene personalisierte Information.

9. Verfahren nach Anspruch 8, wobei die personalisierte Information als Teil der Webseite empfangen wird; und die Webseite und personalisierte Information über eine sichere Verbindung bereitgestellt werden.

10. Verfahren nach Anspruch 8 oder 9, wobei die personalisierte Information vom Nutzer über eine sichere Verbindung bereitgestellt wird.

11. Verfahren nach Anspruch 10, wobei die personalisierte Information einer Datenbank übermittelt wird, die von einer von der die Webseite betreibenden Partei verschiedenen Partei betrieben wird.

12. Verfahren nach einem der vorangehenden Ansprüche, wobei die empfangene Webseite eine Maske zur Eingabe vertraulicher Information umfasst.

13. System zur Bereitstellung einer Webseite mit:
einer Registrierungseinheit (**222**) zum Verknüpfen von personalisierter Information mit einer Nutzerkennung in einer mit einem Datenbankausgang verbundenen Datenbank und zum Bereitstellen der Nutzer-

kennung an einem Ausgang, zumindest als Teil eines Registrierungsverfahrens, das zumindest zum Teil zur Festlegung von personalisierter Information für einen Nutzer durchgeführt wird, um dem Nutzer die wahrnehmbare Authentifizierung wenigstens der Webseite zu ermöglichen;
einer Cookie-Erzeugungseinheit (**230**), die einen mit dem Ausgang der Registrierungseinheit verbundenen Eingang aufweist und zur Bereitstellung der Nutzerkennung in einem Cookie an einem Ausgang geeignet ist;
einer Cookie-Verschlüsselungseinheit (**234**), die einen mit dem Ausgang der Cookie-Erzeugungseinheit verbundenen Eingang aufweist und zur Verschlüsselung des Cookies und der Bereitstellung des verschlüsselten Cookies an einem Ausgang geeignet ist;
einer Cookie-Speichereinheit (**266**), die einen mit dem Ausgang der Cookie-Verschlüsselungseinheit verbundenen Eingang/Ausgang aufweist und zur Speicherung des Cookies auf einem von dem Nutzer betriebenen Rechnersystem geeignet ist;
einer Webanwendungs-Einheit (**240**), die einen zum Empfang einer Anfrage nach einer Webseite angeschlossenen Eingang aufweist und geeignet ist, als Reaktion auf die Anforderung der Webseite den über den Eingang der Webanwendungs-Einheit gespeicherten Cookie auszulesen, an einem ersten Ausgang zumindest einen Teil der Webseite bereitzustellen und an einem zweiten Ausgang die Nutzerkennung aus dem ausgelesenen Cookie bereitzustellen; und
einer Bereitstellungs-Einheit für personalisierte Information (**244**), die zum Empfangen der Nutzerkennung einen an den zweiten Ausgang der Webanwendungs-Einheit gekoppelten Eingang aufweist und dazu geeignet ist, wenigstens einen Teil der personalisierten Information von der Datenbank über einen mit der Datenbank verbundenen Eingang/Ausgang abzurufen, und ferner dazu geeignet ist, als Reaktion auf die Anfrage der Webseite nach vertraulicher Information oder auf die Bereitstellung von Information, für die von dem Nutzer ein Authentifizierungs-Kennzeichen gewünscht werden kann, durch die Webseite an einem Ausgang die personalisierte Information über:
a) eine sichere Verbindung und/oder
b) einen Verbindungskanal, der sich von dem zur Bereitstellung der Webseite benutzten Kanal unterscheidet,
bereitzustellen.

14. System nach Anspruch 13 mit zusätzlich:
einer Cookie-Signatureinheit, die zwischen der Cookie-Erzeugungseinheit und der Cookie-Verschlüsselungseinheit angeschlossen und dazu geeignet ist, dem Cookie eine Signatur des Cookies hinzuzufügen; und
einer Nutzer-Authentifizierungs-Einheit, die einen Eingang zum Empfangen des Cookies von einem Verifikationsausgang der Registrierungseinheit aufweist und dazu geeignet ist, die Signatur des Cookies zu verifizieren und an einem Ausgang als Reaktion auf wenigstens einen Teil des Cookies und der Signatur des Cookies eine Authentifizierungsmeldung bereitzustellen, wobei die Webanwendungs-Einheit dazu eingerichtet ist, als Reaktion auf die an einem Webanwendungs-Authentifizierungs-Eingang, der mit dem Nutzer-Authentifizierungs-Ausgang verbunden ist, empfangene Meldung die Webseite bereitzustellen.

15. System nach Anspruch 13 oder 14, wobei die Bereitstellungseinheit für die personalisierte Information dazu eingerichtet ist, die als Teil der Webseite integrierte personalisierte Information bereitzustellen.

16. System nach Anspruch 13 oder 14, wobei die Bereitstellungseinheit für die personalisierte Information dazu eingerichtet ist, die personalisierte Information im Wesentlichen gleichzeitig mit der Webseite, aber davon getrennt, bereitzustellen.

17. System nach Anspruch 14 oder 15, wobei auf die Datenbank von einem von der Webanwendung entfernten Netzwerk aus zugegriffen wird.

18. Rechnerprogramm-Erzeugnis mit einem von einem Rechner verwendbaren Medium, das einen rechnerlesbaren Programmcode enthält, zur Bereitstellung einer Webseite, wobei das Rechnerprogramm-Erzeugnis rechnerlesbare Programmcode-Mittel umfasst, die dazu eingerichtet sind, einen Rechner zur Ausführung des Verfahrens nach einem der Ansprüche 1 bis 12 zu veranlassen.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

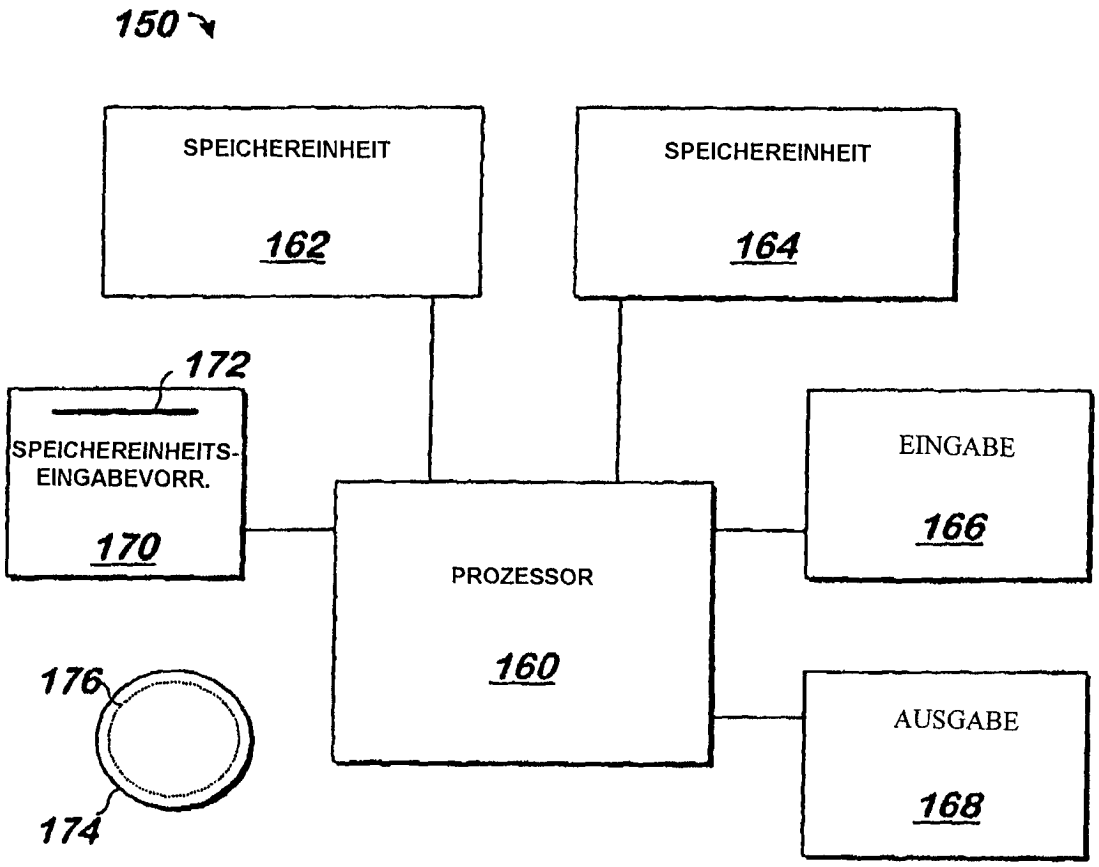

FIG. 1
(STAND DER TECHNIK)

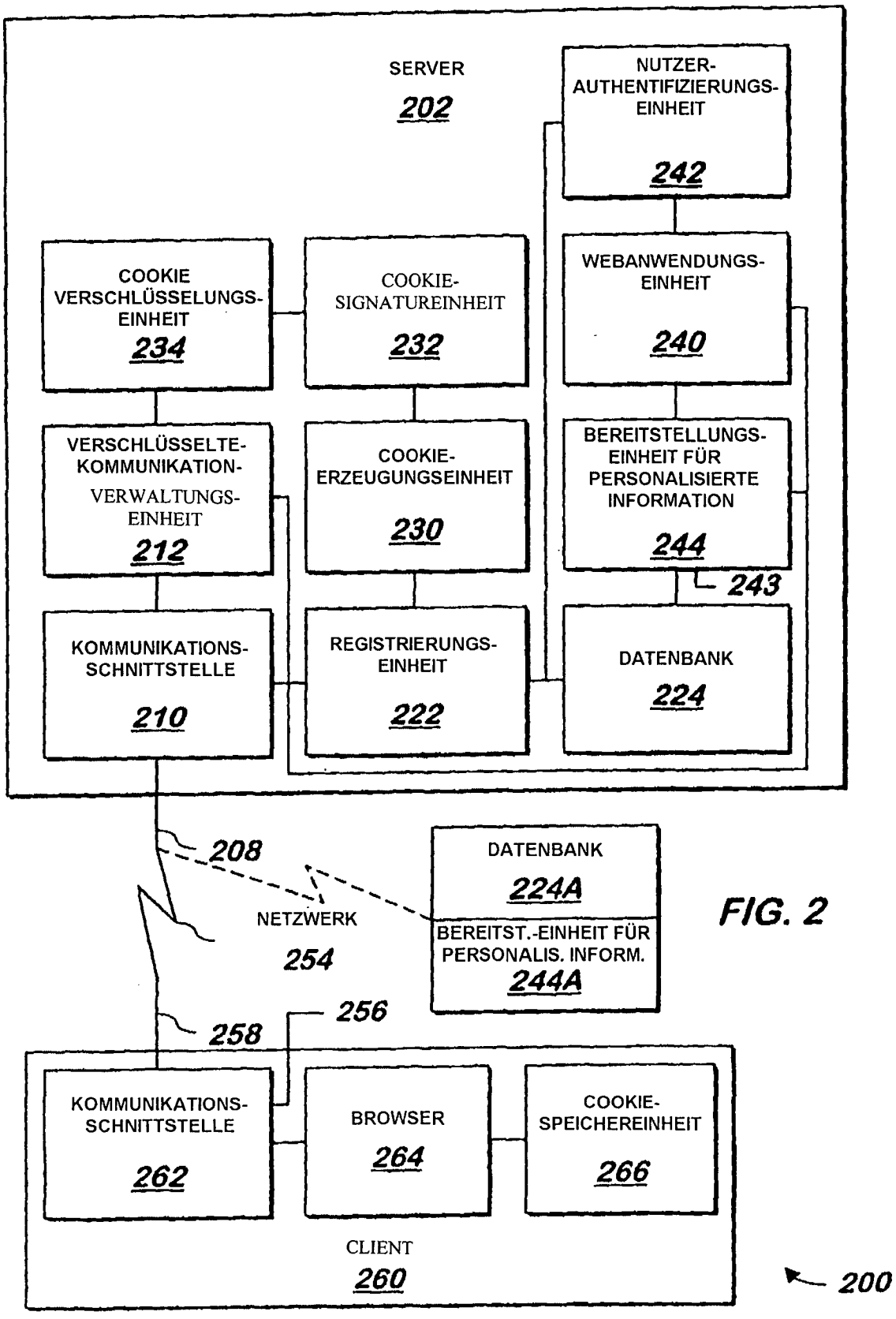
SERVER
202
NUTZER-AUTHENTIFIZIERUNGS-EINHEIT
242
COOKIE VERSCHLÜSSELUNGS-EINHEIT
234
COOKIE-SIGNATUREINHEIT
232
WEBANWENDUNGS-EINHEIT
240
VERSCHLÜSSELTE-KOMMUNIKATION-VERWALTUNGS-EINHEIT
212
COOKIE-ERZEUGUNGSEINHEIT
230
BEREITSTELLUNGS-EINHEIT FÜR PERSONALISIERTE INFORMATION
244
243
KOMMUNIKATIONS-SCHNITTSTELLE
210
REGISTRIERUNGS-EINHEIT
222
DATENBANK
224
208
NETZWERK
254
DATENBANK
224A
BEREITST.-EINHEIT FÜR PERSONALIS. INFORM.
244A
256
258
KOMMUNIKATIONS-SCHNITTSTELLE
262
BROWSER
264
COOKIE-SPEICHEREINHEIT
266
CLIENT
260
200

FIG. 2

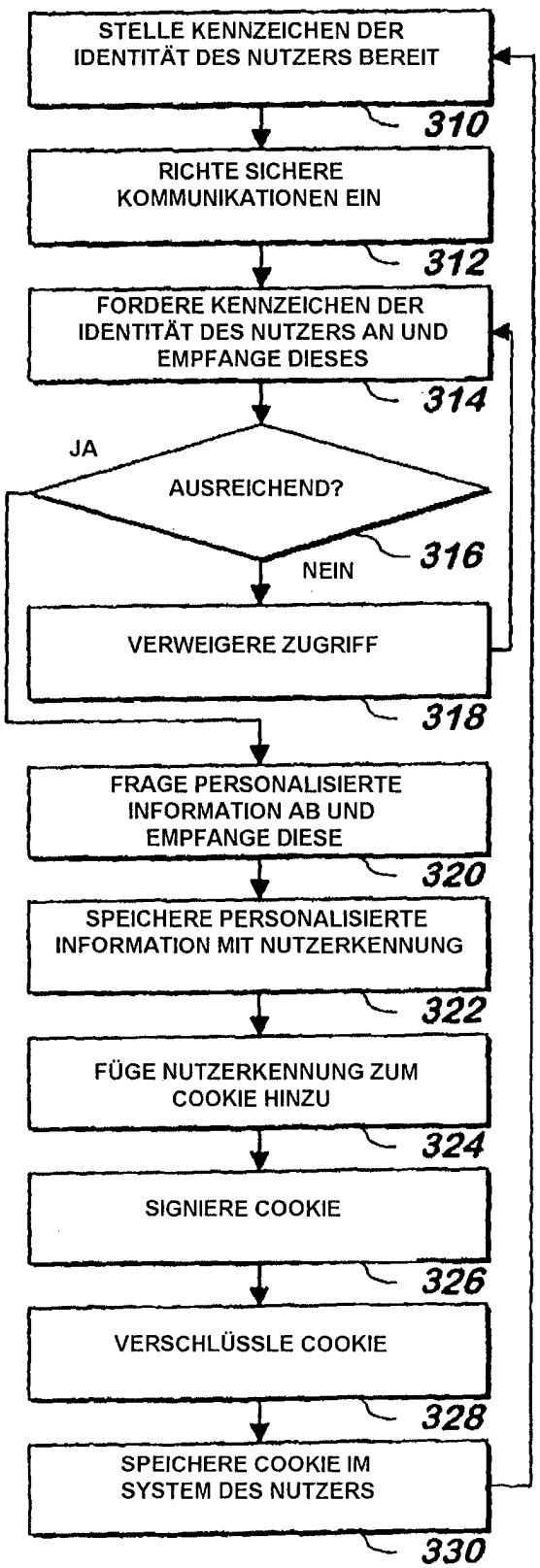
STELLE KENNZEICHEN DER IDENTITÄT DES NUTZERS BEREIT
310
RICHTE SICHERE KOMMUNIKATIONEN EIN
312
FORDERE KENNZEICHEN DER IDENTITÄT DES NUTZERS AN UND EMPFANGE DIESES
314
JA
AUSREICHEND?
316
NEIN
VERWEIGERE ZUGRIFF
318
FRAGE PERSONALISIERTE INFORMATION AB UND EMPFANGE DIESE
320
SPEICHERE PERSONALISIERTE INFORMATION MIT NUTZERKENNUNG
322
FÜGE NUTZERKENNUNG ZUM COOKIE HINZU
324
SIGNIERE COOKIE
326
VERSCHLÜSSLE COOKIE
328
SPEICHERE COOKIE IM SYSTEM DES NUTZERS
330

FIG. 3A

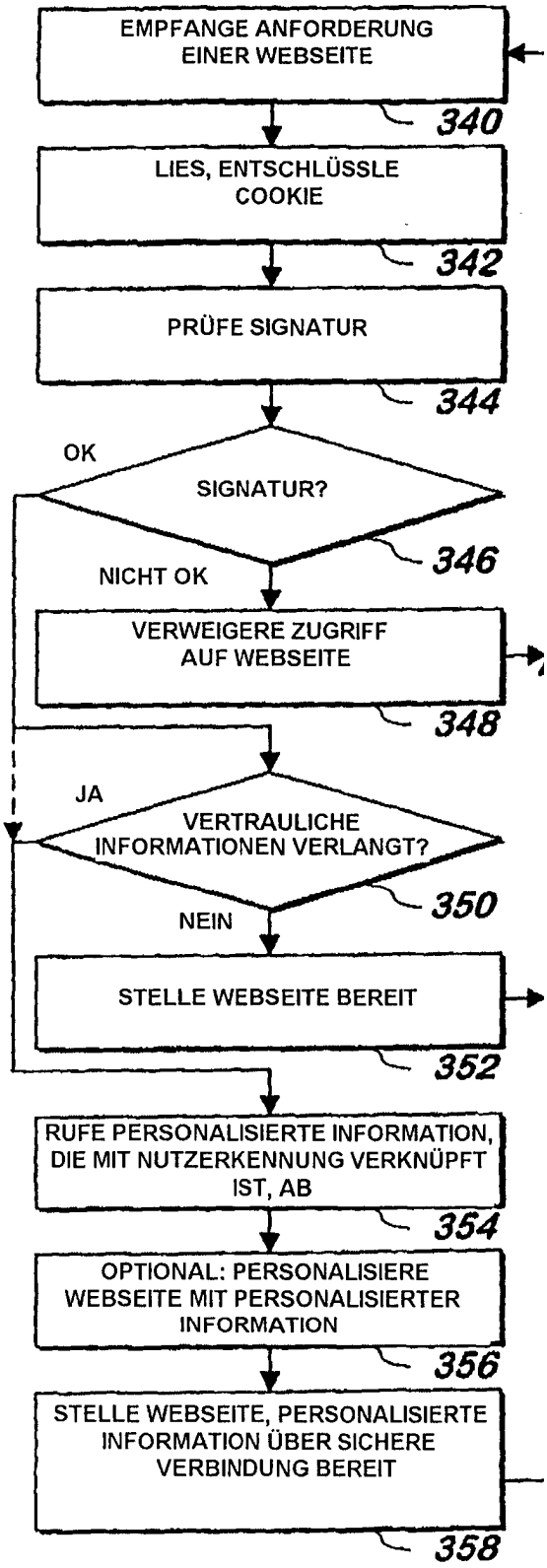
EMPFANGE ANFORDERUNG EINER WEBSEITE
340
LIES, ENTSCHLÜSSLE COOKIE
342
PRÜFE SIGNATUR
344
OK
SIGNATUR?
346
NICHT OK
VERWEIGERE ZUGRIFF AUF WEBSEITE
348
JA
VERTRAULICHE INFORMATIONEN VERLANGT?
350
NEIN
STELLE WEBSEITE BEREIT
352
RUFE PERSONALISIERTE INFORMATION, DIE MIT NUTZERKENNUNG VERKNÜPFT IST, AB
354
OPTIONAL: PERSONALISIERE WEBSEITE MIT PERSONALISIERTER INFORMATION
356
STELLE WEBSEITE, PERSONALISIERTE INFORMATION ÜBER SICHERE VERBINDUNG BEREIT
358

FIG. 3B

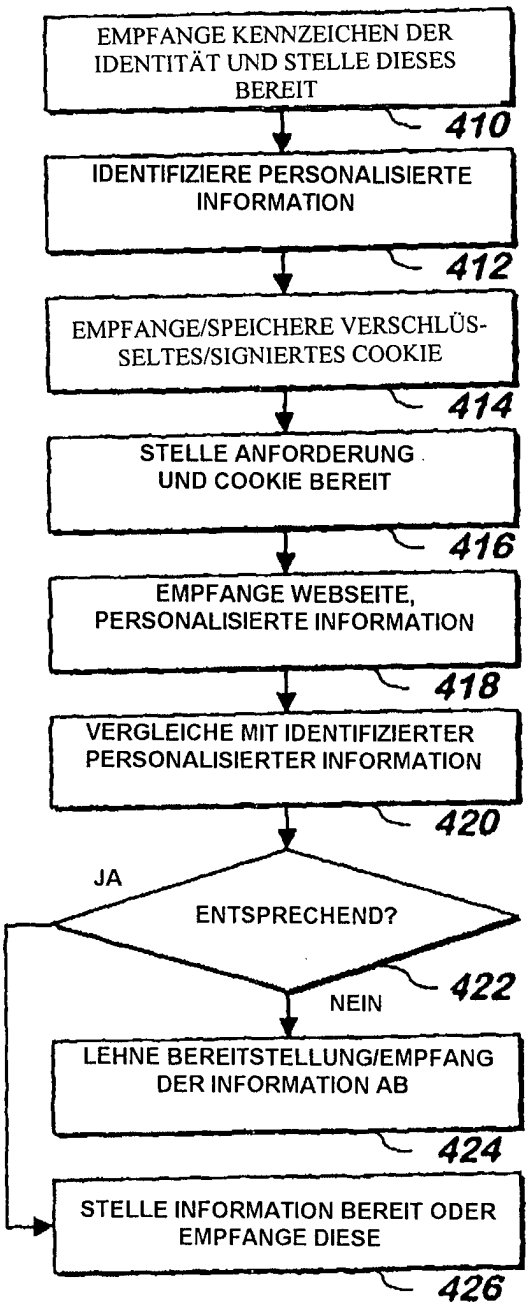
EMPFANGE KENNZEICHEN DER IDENTITÄT UND STELLE DIESES BEREIT
410
IDENTIFIZIERE PERSONALISIERTE INFORMATION
412
EMPFANGE/SPEICHERE VERSCHLÜSSELTES/SIGNIERTES COOKIE
414
STELLE ANFORDERUNG UND COOKIE BEREIT
416
EMPFANGE WEBSEITE, PERSONALISIERTE INFORMATION
418
VERGLEICHE MIT IDENTIFIZIERTER PERSONALISIERTER INFORMATION
420
JA
ENTSPRECHEND?
422
NEIN
LEHNE BEREITSTELLUNG/EMPFANG DER INFORMATION AB
424
STELLE INFORMATION BEREIT ODER EMPFANGE DIESE
426

FIG. 4