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

(10) **DE 603 10 872 T2** 2007.10.18

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 455 290 B1**
(21) Deutsches Aktenzeichen: **603 10 872.5**
(96) Europäisches Aktenzeichen: **03 102 743.6**
(96) Europäischer Anmeldetag: **15.09.2003**
(97) Erstveröffentlichung durch das EPA: **08.09.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **03.01.2007**
(47) Veröffentlichungstag im Patentblatt: **18.10.2007**

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

(30) Unionspriorität:
0211805 **24.09.2002** **FR**

(73) Patentinhaber:
Société Française du Radiotéléphone-SFR, Paris, FR

(74) Vertreter:
Schmit Chretien Schihin & Mahler, 80469 München

(72) Erfinder:
Wary, Jean-Philippe, 92340 Bourg la Reine, FR

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

(54) Bezeichnung: **Verfahren zur Verwaltung einer Einstellung eines Gateways von einem Benutzer des Gateways**

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

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

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Verwaltung einer Verhaltenskonfiguration einer Brücke eines Zugriffsanbieters in Abhängigkeit von den Wünschen eines Benutzers, der auf einen Inhaltsanbieter über die Brücke des Zugriffsanbieters zugreift. Das Gebiet der Erfindung ist jenes des Zugriffsangebots auf Multimedianetze, wie beispielsweise das Internet. Insbesondere ist das Gebiet der Erfindung jenes der Mobiltelefonbetreiber, die es ihren Teilnehmern ermöglichen, auf Inhaltsangebotsserver zuzugreifen. Ein Ziel der Erfindung besteht darin, es einem Benutzer, der an einen Zugriffsanbieter zu einem Multimedianetz angeschlossen ist, zu ermöglichen, seine Privatsphäre zu bewahren. Ein weiteres Ziel der Erfindung besteht darin, es diesem selben Benutzer zu ermöglichen, die Verwaltung seiner Privatsphäre zu parametrieren. Ein weiteres Ziel der Erfindung besteht darin, Kontexte in Abhängigkeit von einer Identität des Benutzers zu verwalten.

[0002] Im Stand der Technik gibt es mehrere Mittel für einen Inhaltsanbieter, um einen Benutzer zu identifizieren, der auf einen seiner Dienste zuzugreifen. Diese Mittel hängen von dem vom Benutzer verwendeten Medium ab, um auf den Dienst zuzugreifen. Es werden hauptsächlich vier Zugriffsarten unterschieden, aber die Liste ist nicht erschöpfend. Eine erste Zugriffsart ist ein Zugriff vom Typ Internet. Der Internet-Modus unterteilt sich selbst in zwei Untermodi, die als angeschlossener Modus und nicht angeschlossener Modus bezeichnet werden können. Der angeschlossene Internet-Modus ist ein Anschlussmodus, der ein Protokoll des Typs HTTP (Hyper Text Transfer Protocol oder Hypertextübertragungsprotokoll) oder WTP (Wireless Transfer Protocol oder drahtloses Übertragungsprotokoll) verwendet. Ein Server, beispielsweise HTTP, ist ein Gerät, das über ein Netz, beispielsweise das Internet, und nach einem HTTP-Protokoll kommuniziert. Ein solcher Server beherbergt WEB-Sites (oder Internet-Sites) oder WAP-Seites (oder an das Mobiltelefon angepasste Internet-Sites). Es gibt auch einen nicht angeschlossenen Internet-Zugriffsmodus über ein Protokoll des Typs SMTP (Simple Mail Transfer Protocol oder einfaches Mailübertragungsprotokoll), bei dem der Anschluss tatsächlich in einem Austausch einer elektronischen Meldung des Typs Mail besteht.

[0003] Ein weiterer Zugriffsmodus ist ein Zugriffsmodus durch einen Betreiber, welcher ebenfalls in zwei Untermodi unterteilt ist. Ein erster Zugriffsuntermodus und dritter Zugriffsmodus ist nun ein Zugriffsmodus, der als nicht angeschlossen über ein Protokoll des Typs SMS (Short Message Service oder Kurzmeldungsdienst) oder MMS (Multimedia Message Service oder Multimediameldungsdienst) bezeichnet werden kann. Ein vierter Zugriffsmodus ist ein Modus durch einen angeschlossenen Betreiber, der auch Vokalmodus genannt wird und bei dem der Benutzer auf einem Vokalserver zugreift.

[0004] Für die vier Zugriffsarten gibt es eine einfache Lösung, die darin besteht, eine Schnittstelle herzustellen, die die Erfassung eines Identifikators und eines Passwortes bei einem Anschluss an einen Server vorschlägt. In dem Maße, als sich der Benutzer an den Server des Inhaltsanbieters anschließt und dies über ein Mobiltelefon tut, sind die Mittel, die dem Benutzer zur Verfügung gestellt werden, um den Identifikator (oder login) und das Passwort zu erfassen, durch die Benutzerschnittstelle des Telefons begrenzt. Entweder sind der Identifikator und das Passwort zur Gänze digital, dann sind sie schwer zu behalten und leicht zu erraten. Oder der Identifikator und das Passwort sind alphanumerisch, in welchem Fall es langwierig ist, sie mit einer Tastatur mit nur 9 Tasten einzugeben. Ferner stellt dieser Eingabeschritt einen zusätzlichen Schritt für den Benutzer dar, weshalb in den meisten Fällen ein Benutzer eines Mobiltelefons davon Abstand nimmt, sich an die Site anzuschließen, die eine Anschlussschnittstelle des Typs Identifikator und Passwort vorschlägt.

[0005] Eine weitere Lösung im Falle der Server des ersten Typs besteht darin, sich eines Cookies oder einer Anzeige zu bedienen. Ein Cookie ist eine kleine Datei, die auf dem Gerät des Benutzers aufgezeichnet ist. Bei einem Anschluss an einen Inhaltsanbieter kann der Inhaltsanbieter nun auf dieses Cookie zugreifen, um den Benutzer zu identifizieren. Ein Problem dieser Lösung besteht in der Tatsache, dass es möglich ist, ein Cookie durch elektronische Mittel oder dergleichen zu stehlen.

[0006] Die Verwendung eines Cookies ist somit nicht mit den strengen Sicherheitsanforderungen vereinbar. Ein weiteres Problem besteht nun in der Tatsache, dass die Cookies eine relativ schlechte Presse haben, was die Benutzer dazu veranlasst, sie zu löschen. Ferner kann der Benutzer die Anwendung oder den Navigator, den er Verwendet, um sich an den Inhaltsanbieter anzuschließen, derart konfigurieren, dass diese Anwendung die Cookies nicht akzeptiert. In diesem Fall ist es dem Benutzer unmöglich, sich an den Server des Inhaltsanbieters anzuschließen.

[0007] Für die zweiten und dritten Servertypen hat der Inhaltsanbieter meistens Zugriff auf die Telefonnummer der Person, die den Server anruft. Der Inhaltsanbieter ist somit in der Lage, die Person über diese Telefonnummer zu identifizieren. Dies geht nicht, ohne ein Problem des Schutzes der Privatsphäre aufzuwerfen. Es ist nämlich absolut vorstellbar, dass ein Benutzer nicht physisch identifiziert werden möchte, wenn er sich an einen Server eines Inhaltsanbieters anschließt. Es ist nun möglich zu versuchen, sich unter Verschleierung seiner Nummer an-

zuschließen, aber in diesem Fall ist es unmöglich, den Dienst zu fakturieren und somit sich anzuschließen. Derzeit besteht die einzige Lösung somit darin, sich nicht an diesen Inhaltsanbieter anzuschließen.

[0008] Im Stand der Technik ist auch das Dokument WO 00/48110A bekannt.

[0009] Es ist somit festzustellen, dass im Stand der Technik entweder der Benutzer, der sich an einen Server eines Inhaltsanbieters anschließt, perfekt über seine Telefonnummer identifiziert ist, oder sich der Benutzer an einen Identifikator und ein Passwort für jeden Inhaltsanbieter erinnern muss. Im ersten Fall kann angenommen werden, dass es sich um einen großen Eingriff in die Privatsphäre des Benutzers handelt, im zweiten Fall entmutigt die Verwaltung aller dieser Identifikatoren sehr oft den Benutzer. Meistens hat dies zur Folge, dass ein Benutzer, der sich mehrmals an eine selbe Site anschließt, bevorzugt, einen neuen Identifikator und ein neues Passwort zu erstellen, da jene, die er bei seinem vorhergehenden Anschluss verwendet hat, vergessen hat.

[0010] Bei der Erfindung werden diese Probleme gelöst, wobei die Verwaltung der Privatsphäre eines an einen Zugriffsanbieter Benutzers auf einer Brücke zentralisiert wird. Diese Brücke verwendet eine Konfigurationsdatei, um das Verhalten zu definieren, das der Teilnehmer von der Brücke erwartet. Diese Konfigurationsdatei ist nach Belieben für den Benutzer zugänglich und veränderbar. Eine solche Konfigurationsdatei ermöglicht es, für jeden Inhaltsanbieter zu definieren, welchen Identifikatortyp der Benutzer dem Inhaltsanbieter vorlegen möchte und bei welchen Diensten der Benutzer akzeptiert, dass sie dem Inhaltsanbieter zur Verfügung gestellt werden.

[0011] Die Identifikatortypen, die die Brücke **103** erzeugen/vorlegen kann, sind Isolieridentifikatoren und befinden sich unter einem temporären Identifikator oder einem Sitzungsidentifikator, der eine auf einige Minuten begrenzte Lebensdauer hat, einem Kontextidentifikator, der eine wesentlich längere Lebensdauer von ungefähr sechs Monaten bis zu mehreren Jahren hat, und einen personalisierten Identifikator, den der Benutzer selbst definiert. Ein Isolieridentifikator isoliert den Zivilstand des Benutzers, der vom Zugriffsanbieter bekannt ist, vom Inhaltsanbieter, der nur den Isolieridentifikator kennt.

[0012] Die Dienste, die die Brücke Inhaltsanbietern zur Verfügung stellen kann, sind Lokalisierungsdienste, Informationsdienste über das vom Benutzer verwendete Gerät, um sich an den Inhaltsanbieter anzuschließen, Portemonnaiedienste, Bankkontodienste, Visitkartendienste, Lieferadressendienste und so weiter.

[0013] Die Erfindung betrifft somit ein Verfahren zur Verwaltung einer Verhaltenskonfiguration einer Brücke eines Zugriffsanbieters in Abhängigkeit von den Wünschen eines Benutzers, der auf einen Inhaltsanbieter über die Brücke des Zugriffsanbieters zugreift, gemäß Anspruch 1.

[0014] Die Erfindung wird durch die Studie der nachfolgenden Beschreibung und der begleitenden Figuren besser verständlich. Diese haben nur hinweisenden und keineswegs für die Erfindung einschränkenden Charakter. Die Figuren zeigen:

[0015] Fig. 1: eine Darstellung von nützlichen Mitteln für den Einsatz des erfindungsgemäßen Verfahrens;

[0016] Fig. 2: eine Darstellung eines Szenarios, das das erfindungsgemäße Verfahren einsetzt.

[0017] Fig. 1 zeigt ein Gerät **101**, das es einem Benutzer ermöglicht, sich an einen Server **102** eines Inhaltsanbieters über eine Brücke **103** eines Zugriffsanbieters zu einem Multimedianetz **104** anzuschließen.

[0018] Für die Beschreibung wird angenommen, dass das Gerät **101** ein Mobiltelefon **101** ist. Dieser schließt sich somit an eine Basisstation **105** über eine Funkverbindung **106** eines zellulären Mobiltelefonnetzes an. Die Basisstation **105** ist an die Brücke **103** des Zugriffsanbieters angeschlossen. In dem Beispiel ist der Zugriffsanbieter auch Mobiltelefonbetreiber, und dieser Betreiber verwaltet die Basisstation **105**.

[0019] In der Beschreibung wird angenommen, dass das Netz **104** das Internet ist. In der Praxis könnte es sich um jedes beliebige Netz handeln, das es ermöglichet, den Server **102** des Inhaltsanbieters an die Brücke **103** anzuschließen. Ein solches Netz könnte sehr gut beispielsweise ein Telefonwählnetz sein.

[0020] Auf dem zellulären Telefonnetz wird der Benutzer des Mobiltelefons **101** durch einen Benutzeridentifikator identifiziert, der seine Telefonnummer ist. Diese Telefonnummer ermöglicht es somit jedem, diesem Benutzeridentifikator eine physische Person zuzuordnen. Durch diesen Benutzeridentifikator wird der Benutzer nämlich mit seinem Telefon verbunden.

[0021] Fig. 1 zeigt, dass die Brücke **103** einen Mikroprozessor **107** umfasst. Die Brücke **103** umfasst auch Schnittstellenschaltungen **108** mit der Basisstation **105**. Die Schaltungen **108** sind an den Mikroprozessor über einen Bus **109** angeschlossen.

[0022] Die Brücke **103** umfasst auch Schnittstellenschaltungen **110** mit dem Internet **104**. Die Schaltungen **110** sind an den Bus **109** angeschlossen. Die

Rolle der Schnittstellenschaltungen besteht darin, eine Kompatibilität der Signale zwischen dem Äußeren der Brücke **103** und den auf dem Bus **109** zirkulierenden Signalen zu sichern.

[0023] Die Brücke **103** umfasst auch einen Programmspeicher **111**. Der Speicher **111** umfasst Befehlscodes, die es der Brücke **103**, d.h. dem Mikroprozessor **107**, ermöglichen, Aktionen durchzuführen. Der Speicher **111** umfasst eine Zone **111a**, die Befehlscodes für die Codierung und Decodierung der Identifikatoren umfasst. Der Speicher **111** umfasst auch eine Zone **111b** für die Validierung der Identifikatoren. Kurz ermöglicht es die Zone **111a** hier, den Schutz der Privatsphäre eines Benutzers zu sichern, wobei der Benutzeridentifikator in einen Isolierbenutzeridentifikator umgewandelt wird. Die Zone **111b** ermöglicht es der Brücke **103**, die Wünsche des Benutzers im Hinblick auf den Umgang mit seiner Privatsphäre zu berücksichtigen.

[0024] Die Brücke **103** umfasst auch einen Benutzerspeicher **112**. Der Speicher **112** ist, wie der Speicher **111**, an den Bus **109** angeschlossen. Der Speicher **112** ist tatsächliche eine Benutzerdatenbasis, die zumindest die Informationen zur Verwaltung der Privatsphäre der Benutzer umfasst. Der Speicher **112** ist für die Zwecke der Beschreibung in Registrierungen unterteilt. Eine Registrierung kann eine Datei oder ein Teil einer Datei in einem digitalen Speicher sein. Es gibt somit vorzugsweise im Speicher **112** ebenso viele Registrierungen wie Benutzer, die die Brücke **103** verwenden können, um sich an einen Inhaltsanbieter anzuschließen. Jede Registrierung entspricht nun einem Benutzer/Teilnehmer. Jedoch kann es sein, dass ein Benutzer/Teilnehmer nicht mit einer Registrierung verbunden ist. In diesem Fall gibt es eine Fehlregistrierung, die allen Benutzern/Teilnehmern zugeordnet ist, die keine eigene Registrierung im Speicher **112** haben. Es wird nur die Struktur einer Registrierung **112a** beschrieben, da alle Registrierungen dieselbe Struktur haben.

[0025] Eine Registrierung **112a** umfasst ein erstes IDU-Feld, das es ermöglicht, den Benutzeridentifikator zu registrieren. Das IDU-Feld umfasst somit vorzugsweise eine Telefonnummer eines Benutzers, der an den Betreiber, der die Brücke **103** verwaltet, angeschlossen ist.

[0026] Das IDU-Feld ermöglicht den Zugriff auf die richtige Registrierung. Eine Registrierung **112a** umfasst eine Tabelle **113**. Die Tabelle **113** ist in Zeilen und Spalten gegliedert. Jede Zeile entspricht einem Inhaltsanbieter, und jede Spalte entspricht einer Information über den Inhaltsanbieter. Die Tabelle **113** umfasst eine Spalte **113a**, die es ermöglicht, einen Identifikator eines Inhaltsanbieters zu registrieren. Ein solcher Identifikator eines Inhaltsanbieters ist beispielsweise eine Internet-Adresse oder eine URL (Universal Resource Locator für universelle Ressourcenlokalisierung), eine Telefonnummer, eine IP-Adresse, im Allgemeinen eine elektronische Adresse.

[0027] Die Tabelle **113** umfasst eine zweite Spalte **113b**, die der Art des Isolieridentifikators entspricht, die der Benutzer dem Inhaltsanbieter zuordnet. Eine Spalte **113c** ermöglicht es dem Benutzer, eine Dienstleistungsliste dem Inhaltsanbieter zuzuordnen. Die in dieser Liste enthaltenen Dienste sind jene, die die Brücke dem Inhaltsanbieter erweisen darf, wenn ein Dienstleistungsantrag den Benutzer, der vom IDU-Feld identifiziert wurde, betrifft.

[0028] Die Brücke **103** hat somit eine Zwischenrolle zwischen dem Gerät **101** und dem Server **102**. Im Allgemeinen empfängt und/oder entsendet die Brücke **103** Raster **114** von und/oder zu dem Gerät **101**. Ein Raster **114** umfasst zusätzlich Daten, die für die Kommunikation Zugriffsanbieter/Benutzer nützlich sind, ein Feld **115**, das den Benutzer identifiziert, ein Feld **116**, das den Inhaltsanbieter identifiziert, und ein Feld **117** von transportierten Daten. Die Brücke **103** empfängt und/oder entsendet andererseits Raster **118** von und/oder zu dem Server **102**. Der Raster **118** umfasst zusätzlich Daten, die für die Kommunikation Zugriffsanbieter/Inhaltsanbieter nützlich sind, ein Benutzeridentifikationsisolierfeld **119**, ein Feld **120**, das den Inhaltsanbieter identifiziert, und ein Feld **121** von transportierten Daten. Die Brücke **103** ermöglicht es über die Befehlscodes der Zone **111a**, eine Verbindung zwischen einerseits den Feldern **115**–**116** und andererseits dem Feld **119** herzustellen. In der Praxis sind die Felder **116** bzw. **117** identisch mit den Feldern **120** bzw. **121**.

[0029] Fig. 2 zeigt einen vorherigen Schritt **201**, bei dem der Benutzer des Geräts **101** dieses Gerät verwendet, um eine Anfrage an einen Inhaltsanbieter zu richten. Für das Beispiel wird angenommen, dass die in Schritt **201** entsandte Anfrage eine Anfrage des Typs GET ist oder einem Protokoll des Typs HTTP entspricht, d.h. Hypertext Transfer Protocol oder Hypertexttransferprotokoll. Die Anfrage des Schrittes **201** oder UGET-Anfrage wird somit vom Gerät **101** entsandt und in Schritt **203** von der Brücke **103** empfangen. Die UGET-Anfrage ist vom Typ der Anfrage des Rasters **114**.

[0030] In Schritt **203** hat die Brücke **103** Zugriff auf den Benutzeridentifikator **115** der UGET-Anfrage. Dieser Benutzeridentifikator **115** ermöglicht es dem Mikroprozessor **107**, eine Registrierung im Speicher **112** wieder zu finden. Andererseits hat der Mikroprozessor **107** dank der UGET-Anfrage Zugriff auf den Identifikator **116** des Inhaltsanbieters. Dies ermöglicht es, eine Zeile in der Tabelle **113** zu identifizieren. Diese identifizierte Zeile informiert nun über die Art des Isolieridentifikators, den die Brücke **103** erzeu-

gen soll. Es wird nun in einen Schritt **204** der Bestimmung der Art des zu erzeugenden Isolieridentifikators übergegangen. In Schritt **204** des Beispiels gibt es vier Möglichkeiten. Eine erste Möglichkeit **204.1** entspricht einer Art eines temporären oder Sitzungsisolieridentifikators. Ein Schritt **204.2** entspricht einer Art eines permanenten oder Kontextidentifikators. Ein Schritt **204.3** entspricht einer Art eines personalisierten Identifikators. Schließlich entspricht ein Schritt **204.4** einer Art eines Fehlidentifikators. Der Schritt **204.x**, der eingesetzt wird, wird durch das Vorhandensein oder nicht des Identifikators **116** in der Tabelle **113** bestimmt. Wenn der Identifikator **116** nicht in der Tabelle **113** vorhanden ist, wird eine spezifische Zeile der Tabelle **113** verwendet, die dem Fehlverhalten entspricht. Wenn der Identifikator **116** des Inhaltsanbieters in der Tabelle **113** vorhanden ist, informiert nun das Feld **113b** über die Art des Identifikators und somit über den eingesetzten Schritt **204.1**–**204.3**.

[0031] Von Schritt **204.1** wird in einen Schritt **205** der Erzeugung eines IGET-Rasters mit einem temporären Identifikator übergegangen, von Schritt **204.2** wird in einen Schritt **206** der Erzeugung eines IGET-Rasters mit einem permanenten Identifikator übergegangen, von Schritt **204.3** wird in einen Schritt **207** der Erzeugung eines IGET-Rasters mit einem personalisierten Identifikator übergegangen. Von Schritt **204.4** wird ein IGET-Raster mit einem Identifikator erzeugt, der der Art des in der Tabelle **113** spezifizierten Fehlidentifikators entspricht.

[0032] In den Schritten **205** bis **207** erzeugt die Brücke **103** einen IGET-Raster, der dem Raster **118** entspricht. Was die Schritte **205** bis **207** unterscheidet, ist die Art des Benutzerisolieridentifikators, der erzeugt wird, um das Feld **119** zu informieren.

[0033] Ein temporärer Identifikator ist beispielsweise ein Datum, das einem Benutzeridentifikator zugeordnet ist. Ein solches Datum ist beispielsweise die UNIX-Zeit, auch unter der Bezeichnung UNIX-timestamp bekannt. Es handelt sich um die Anzahl von abgelaufenen Sekunden seit 1. Januar 1970 0h00. Ein solches Datum, das dem Benutzeridentifikator **115** zugeordnet und dann chiffriert wird, ermöglicht es, ein Identifikationsfeld über einen Benutzerisolieridentifikator zu informieren.

[0034] In Schritt **206** entspricht das erzeugte Benutzerisolieridentifikationsfeld beispielsweise dem Feld **115**, das nach einem bekannten Algorithmus nur der Brücke **103** chiffriert ist. Bei einer Variante ist das Feld **115** vor der Chiffrierung einem Code eines Inhaltsanbieters zugeordnet, der dem Identifikator **116** des Inhaltsanbieters entspricht. So wird ein Identifikationsfeld für den Benutzerisolieridentifikator erhalten, das sowohl vom Benutzer als auch vom Inhaltsanbieter, an den er sich anschließen möchte, abhängt.

[0035] In Schritt **207** entspricht das Identifikationsfeld des Benutzerisolieridentifikators nun einem vom Benutzer spezifizierten Wert.

[0036] In Schritt **206** ist ein Code eines Inhaltsanbieters einem Identifikator eines Inhaltsanbieters über beispielsweise eine nicht in Fig. 1 dargestellte Tabelle zugeordnet.

[0037] Wenn das Identifikationsfeld des Benutzeridentifikators erzeugt ist, wird der Benutzeridentifikator vorzugsweise durch ein Feld vervollständigt, das die Art des Isolieridentifikators anzeigt, und durch ein Feld, das den Betreiber, der den Identifikator erzeugt hat, angibt. Die beiden letztgenannten Felder sind optional, ermöglichen es aber dem Inhaltsanbieter, über den Server **102**, die Benutzerisolieridentifikatoren besser zu verwalten.

[0038] Von den Schritten **205** bis **207** wird in einen Schritt **208** des Empfangs des IGET-Rasters durch den Server **102** übergegangen. In Schritt **208** hat der Server **102** Zugriff auf das Feld **119**. Dies ermöglicht es ihm, eine Tabelle **122** zu konsultieren. Diese Tabelle **122** ist eine Benutzertabelle. Sie ist in Zeilen und Spalten unterteilt. Jede Zeile entspricht einem durch einen Benutzerisolieridentifikator identifizierten Benutzer, jede Spalte entspricht einer Information über den Benutzer.

[0039] In dem Beispiel ist zu sehen, dass das einzige Mittel für den Inhaltsanbieter, um Informationen einem Benutzer zuzuordnen, ist, dies über einen Benutzerisolieridentifikator zu tun. Nun ist die einzige Einheit, die den Benutzerisolieridentifikator einem physischen Benutzer zuordnen kann, der Zugriffsanbieter über die Brücke **103**. Die Privatsphäre des Benutzers ist somit gut durch den Zugriffsanbieter geschützt. Der Inhaltsanbieter muss sich auf einen Isolieridentifikator beschränken, der sich auf einen einzigen Benutzer für die Lebensdauer des Isolieridentifikators bezieht, wobei dieser Isolieridentifikator nun eine Person nur formell und nicht zivil identifiziert. Der Inhaltsanbieter weiß somit nicht, wer sich an seinen Server anschließt. Der Benutzer hat somit die Sicherheit, dass der Inhaltsanbieter nur die Informationen kennt, die der Benutzer selbst und ausdrücklich beim Inhaltsanbieter bei einem Anschluss mitgeteilt hat, der unter Verwendung eines Isolieridentifikators erfolgt ist. Die gesammelten Informationen werden nun nur einem Isolieridentifikator zugeordnet.

[0040] In Schritt **208** kann der Server **102** Informationen in der Tabelle **122** registrieren und/oder eine IREP-Antwort in Richtung des Benutzers erstellen. Die IREP-Antwort ist nun die Antwort auf die erhaltene IGET-Anfrage, wobei die IGET-Anfrage selbst eine Umsetzung der UGET-Anfrage ist.

[0041] Von Schritt **208** wird in einen Schritt **209** des Empfangs/der Übersetzung des Rasters IREP in einen Raster UREP durch die Brücke **103** übergegangen. Dieser Schritt **209** der Übersetzung entspricht der Umwandlung des Benutzerisolieridentifikators in einen Benutzeridentifikator. Dann wird der Raster nun auf das Gerät **101** übertragen. In Schritt **210** empfängt das Gerät **101** den UREP-Raster, eine Antwort auf den UGET-Raster.

[0042] In dem Maße, als ein Benutzerisolieridentifikator von der Brücke **103** erzeugt wurde oder ein Feld dieser Art umfasst, ist die Brücke **103** in der Lage, den Vorgang, der den Benutzerisolieridentifikator erzeugt hat, umzukehren. Nur die Einheit, die den Benutzerisolieridentifikator erzeugt hat, kann die Umkehr durchführen. Diese Umkehr ermöglicht den Zugriff auf einen Benutzeridentifikator, somit auf eine Registrierung im Speicher **112**. Im Falle eines temporären Benutzerisolieridentifikators ermöglicht diese Umkehr den Zugriff auf ein Datum, ermöglicht es somit, das Datum der Erzeugung des temporären Benutzerisolieridentifikators und somit seine Gültigkeit in Abhängigkeit von einer maximalen Lebensdauer für einen solchen Identifikator zu bestimmen.

[0043] Ausgehend von einem Benutzerisolieridentifikator kann der Inhaltsanbieter in einem Schritt **211** über den Server **102** eine ISERVICE-Dienstanfrage entsenden. Diese Dienstanfrage ist nun vom Typ der Anfrage **118**. Die ISERVICE-Anfrage wird von der Brücke **103** in Schritt **212** erhalten.

[0044] Ausgehend von der ISERVICE-Anfrage kann die Brücke **103** einen Benutzerisolieridentifikator wiedergewinnen. Ausgehend von dem Benutzerisolieridentifikator kann die Brücke **103** dank der Befehlscodes der Zone **111a** einen Benutzeridentifikator erzeugen und somit eine Registrierung in der Tabelle **112** bestimmen.

[0045] Das **120** des ISERVICE-Rasters ermöglicht es der Brücke **103**, eine Zeile in der Tabelle **113** entsprechend dem vom Feld **119** identifizierten Benutzer zu bestimmen, wobei es sich um den Schritt **213** der Bestimmung des Inhaltsanbieters handelt. Wenn der Identifikator des Inhaltsanbieters in der Tabelle **113** vorhanden ist, kann der Mikroprozessor **107** nun eine Liste von autorisierten Dienstleistungen für den Inhaltsanbieter dank der Spalte **113c** bestimmten, und es wird in einen Schritt **215** der Validierung der erforderlichen Dienstleistung übergegangen. Wenn der Identifikator des Inhaltsanbieters nicht in der Tabelle **113** ist, wird in einen Schritt **214** der Wiedergewinnung der Liste der autorisierten Fehldienstleistungen übergegangen, die als Liste der für die ISERVICE-Anfrage autorisierten Dienstleistungen dient. Von Schritt **214** wird in den Schritt **215** übergegangen. Falls die Liste der Fehldienstleistungen alle möglichen Dienste umfasst, werden zusätzliche Riegel vorgesehen, die einer eigenen Politik des Zugriffsanbieters entsprechen. Wenn somit alle Dienste oder gewisse vordefinierte Dienste im Fehlmodus aktiviert werden, kann eine Bedingung zur Art des Isolieridentifikators oder des Identifikators des Inhaltsanbieters erstellt werden, um beispielsweise auf den Lokalisierungsdienst zugreifen zu können. Eine Lokalisierung wird nun nur geliefert, wenn der Isolieridentifikator beispielsweise ein temporärer Identifikator ist. Diese zusätzlichen Riegel können von Benutzer zu Benutzer durch eine ausdrückliche Aktion des betreffenden Benutzers weggelassen werden. Ein Riegel ist somit ein Test, der zur Art des Isolieridentifikators oder zum Wert des Identifikators des Inhaltsanbieters in Schritt **214** durchgeführt wird. Dieser Test kann beliebig vom Benutzer deaktiviert werden. Dieser Riegel ist durch ein RIEGEL-Feld einer Tabelle **112.x** verwirklicht. Die Tatsache, dass ein Eingreifen des Benutzers für die Aktualisierung dieses RIEGEL-Feldes erforderlich ist, bewirkt, dass der Benutzer nicht vorgeben kann, über das von der Brücke angenommene Verhalten nicht informiert gewesen zu sein, da er selbst dieses Verhalten parametriert hat. Bei einer Variante unterteilt sich das RIEGEL-Feld in ebenso viele Felder wie Dienstleistungen, die von der Brücke zur Verfügung gestellt werden können.

[0046] Um alle Dienste zu bezeichnen, wird entweder eine Liste definiert, deren Elemente gezählt werden können, und somit ist die Gesamtanzahl von Dienstleistungen bekannt und kann bestimmt werden, ob eine Liste alle Dienstleistungen enthält.

[0047] Oder es wird ein vordefinierter Code verwendet, der für die Bezeichnung aller Dienstleistungen steht.

[0048] Die ISERVICE-Anfrage umfasst in ihrem Feld **121** einen Dienstleistungsidentifikator. Die Brücke **103** bestimmt nun, ob dieser Dienstleistungsidentifikator in der Liste der autorisierten Dienste vorhanden ist. Es handelt sich um Schritt **215**. Wenn der Dienst nicht autorisiert ist, wird in einen Schritt **217** der Beendigung übergegangen, und es erfolgt keine Antwort oder nur eine negative Antwort auf die in Schritt **211** entsandte ISERVICE-Anfrage. Wenn der Dienst autorisiert ist, wird in einen Schritt **216** übergegangen, in dem die Brücke **103** eine Antwort erzeugt oder Aktionen unternimmt, die den vom Server **102** geforderten Dienstleistungen entsprechen.

[0049] In einem Schritt **218** empfängt der Server **102** die Antwort auf die in Schritt **211** entsandte Anfrage.

[0050] In der Praxis sind die verwendeten Chiffrieralgorithmen symmetrische Algorithmen mit Geheimschlüsseln. In dieser Familie sind die Algorithmen DES (Data Encryption Standard für Standarddatenchiffrierung), 3DES, AES (Advanced Encryption

Standard für fortgeschrittener Chiffrierstandard) bekannt. Es gibt weitere, die alle ebenfalls gültig sind.

[0051] Ein Benutzer, der an einen Betreiber, der die Brücke **103** verwaltet, angeschlossen ist, kann sich an die Brücke anschließen, um den Inhalt der Registrierung des ihm entsprechenden Speichers **112** zu aktualisieren. Der Betreiber entscheidet über die Zugriffspolitik zu den Registrierungen. Der Zugriff kann frei sein oder der Quittierung einer Berechtigung unterliegen. Ebenso kann der Zugriff über eine Schnittstelle erfolgen, die es dem Benutzer ermöglicht, sich direkt an die Brücke **103** anzuschließen, oder über eine schriftliche oder mündliche Anfrage an eine Person, die mit der Wartung des Speichers **112** beauftragt ist.

[0052] Eine solche Aktualisierung läuft beispielsweise folgendermaßen ab: ein Benutzer sendet zu der Brücke **103** eine Fernladeanfrage der ihm entsprechenden Registrierung. Wenn der Benutzer autorisiert ist, eine solche Anfrage zu entsenden, umfasst nun die Antwort auf die Anfrage eine Datei, die der angeforderten Registrierung entspricht. Der Benutzer gibt nun die angeforderte Registrierung auf dem Gerät **101** aus. Wenn die Ausgabe beendet ist, wird die ausgegebene Registrierung an die Brücke **103** zur Aktualisierung des Speichers **112** zurückgesandt. Diese Aktualisierung unterliegt ebenfalls einer Berechtigung. Diese Berechtigungen werden von der Brücke **103** in Abhängigkeit von einem Benutzeridentifikator verwaltet.

[0053] Bei einer Variante der Erfindung sind die Registrierungen des Speichers **112** auf den Geräten der Teilnehmer des Betreibers, der die Brücke **103** verwaltet, verteilt. Wenn der Mikroprozessor **107** eine Registrierung konsultieren möchte, muss er eine Anfrage dazu an das Gerät richten, auf dem die Registrierung gespeichert ist, d.h. an das Gerät des Benutzers.

[0054] Bei einer Variante ist die Benutzerdatenbasis **112** nicht auf der Brücke **103** registriert, sondern in einem Speicher eines weiteren Servers, der nicht dargestellt ist und nun von der Brücke **103** abgefragt werden kann.

Patentansprüche

1. Verfahren zur Verwaltung einer Verhaltenskonfiguration einer Brücke eines Zugriffsanbieters in Abhängigkeit von den Wünschen eines Benutzers, der auf einen Inhaltsanbieter über eine Brücke des Zugriffsanbieters zugreift, **dadurch gekennzeichnet**, dass es die folgenden Schritte umfasst:
– die Brücke empfängt (**203**) eine Anfrage des Benutzers,
– die Brücke greift (**204.1**–**204.3**) auf eine Benutzerregistrierung zu, umfassend die Beschreibung des Verhaltens, das der Benutzer von der Brücke erwartet, in Abhängigkeit von einem Identifikator des Inhaltsanbieters,
– die Brücke greift (**204.1**–**204.3**) auf die Benutzerregistrierung über einen ersten Benutzeridentifikator zu, der automatisch im Netz identifiziert und vom Zugriffsanbieter geliefert wird, wenn der Benutzer eine Anfrage an den Inhaltsanbieter richtet,
– im Falle eines Misserfolgs greift die Brücke (**204.3**) auf einen Benutzerspeicher zu, der in Registrierungen unterteilt ist und eine Fehlregistrierung in Verbindung mit allen Benutzern, die keine Benutzerregistrierung besitzen, umfasst, wobei die Brücke nun automatisch auf diese Fehlregistrierung ohne Intervention des Benutzers zugreift,
– die Brücke greift (**209**, **212**) auf die Benutzerregistrierung über einen zweiten isolierenden Benutzeridentifikator beim Erhalt einer Dienstanfrage hinsichtlich des Benutzers seitens eines Inhaltsanbieters zu, um den ersten und den zweiten Identifikator zu verbinden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Benutzerregistrierung den ersten Benutzeridentifikator mit mindestens einem Identifikator eines Inhaltsanbieters verbindet, wobei ein Identifikator eines Inhaltsanbieters mit einer Natur für den zweiten isolierenden Identifikator, der an den Inhaltsanbieter zu liefern ist, verbunden ist, wenn es zu einer Relaisschaltung einer Anfrage des Benutzers an den Inhaltsanbieter durch den Zugriffsanbieter kommt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Natur des zweiten isolierenden Identifikators in mindestens der Gruppe ausgewählt wird, die von temporären, permanenten oder personalisierten Identifikatoren gebildet ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, das eine Benutzerregistrierung den ersten Benutzeridentifikator mit mindestens einem Identifikator eines Inhaltsanbieters verbindet, wobei ein Identifikator eines Inhaltsanbieters mit mindestens einem Dienst verbunden ist, für den der Zugriffsanbieter nun die Erlaubnis hat, ihn dem Inhaltsanbieter zur Verfügung zu stellen.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass eine Benutzerregistrierung eine Beschreibung eines Fehlverhaltens für die Brücke in einer spezifischen Linie einer Tabelle in dem Benutzerspeicher umfasst, wobei das Fehlverhalten von der Brücke übernommen wird, wenn es nicht möglich ist, den Benutzer mit einem Inhaltsanbieter zu verbinden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Benutzerregistrierung in einer Benutzerdatenbasis aufgezeichnet ist,

die von der Brücke abgefragt wird.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass sich der Benutzer an die Benutzerdatenbasis anschließt, um die ihn betreffende Registrierung zu aktualisieren.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Benutzerregistrierung in einem Terminal des Benutzers aufgezeichnet ist, wobei die Brücke dieses Terminal abfragt, um die Benutzerregistrierung zu erhalten.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass ein Fehlverhalten der Brücke durch einen Riegel verriegelt wird, der ausdrücklich vom Benutzer geöffnet werden muss.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

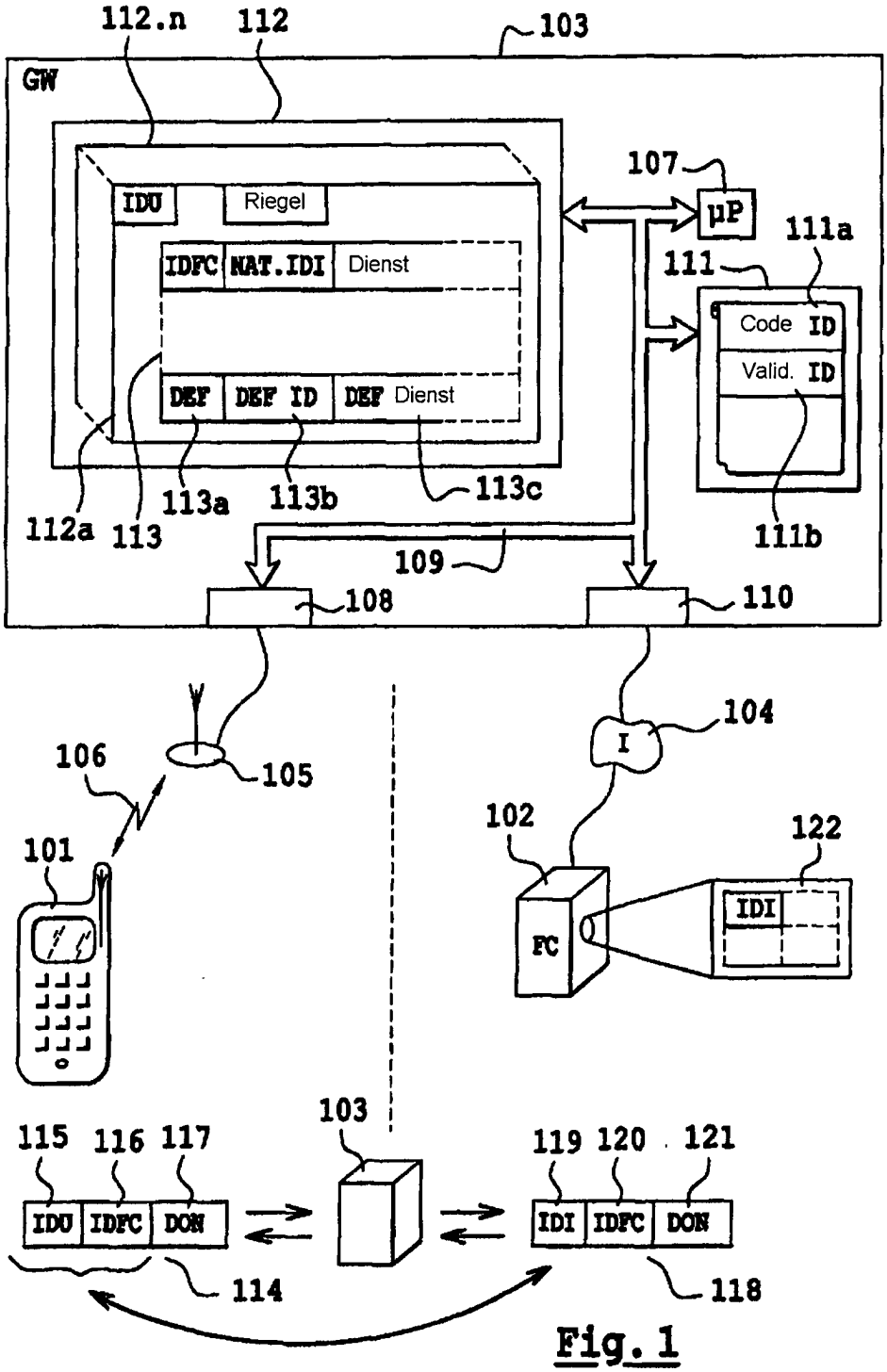


Fig. 1

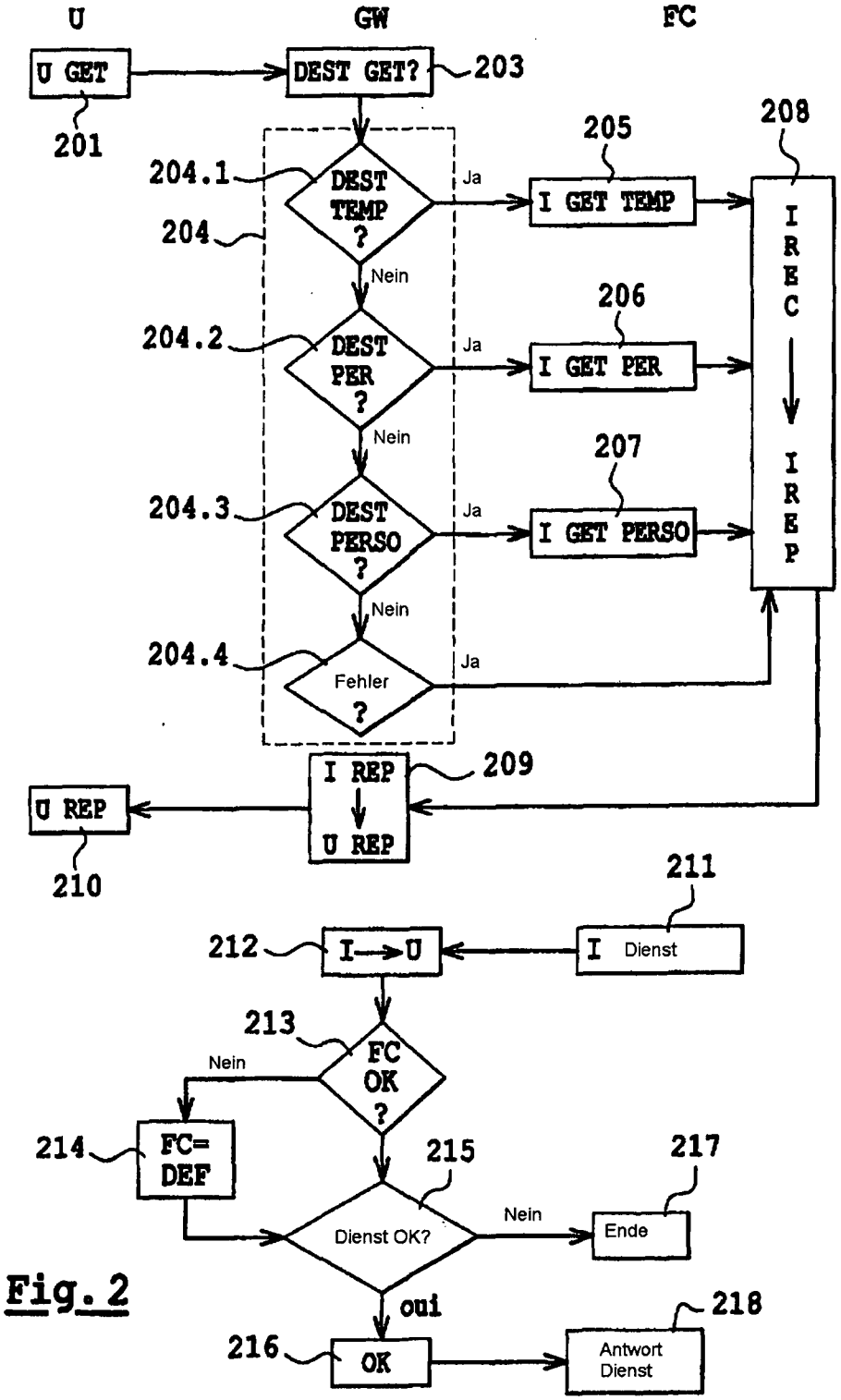

U
GW
FC
U GET
201
DEST GET?
203
204.1
DEST TEMP ?
204
Ja
205
I GET TEMP
208
Nein
204.2
DEST PER ?
Ja
206
I GET PER
Nein
204.3
DEST PERSO ?
Ja
207
I GET PERSO
Nein
204.4
Fehler ?
Ja
I REC
I REP
I REP
U REP
209
U REP
210
211
212
I→U
I Dienst
213
FC OK ?
Nein
214
FC= DEF
215
217
Dienst OK?
Nein
Ende
oui
218
216
OK
Antwort Dienst

Fig. 2