(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Dezember 2012 (20.12.2012)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2012/171568 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04N 21/258* (2011.01)
H04L 29/08 (2006.01) *H04N 21/441* (2011.01)

(21) Internationales Aktenzeichen: PCT/EP2011/060044

(22) Internationales Anmeldedatum:
16. Juni 2011 (16.06.2011)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **TEVEO INTERACTIVE GMBH** [DE/DE]; Klein Fontenay 1, 20354 Hamburg (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **WAGNER, Matthias** [DE/DE]; Großendorferstr. 82, 25355 Barmstedt (DE). **KARANAS, Andreas** [DE/DE]; Orchideenstieg 17, 22297 Hamburg (DE).

(74) Anwalt: **STORK BAMBERGER PATENTANWÄLTE**; Postfach 73 04 66, 22124 Hamburg (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD AND APPARATUS FOR AUTHENTICATING USERS OF A HYBRID TERMINAL

(54) **Bezeichnung** : VERFAHREN UND VORRICHTUNG ZUR AUTHENTIFIZIERUNG VON BENUTZERN EINES HYBRIDENDGERÄTES

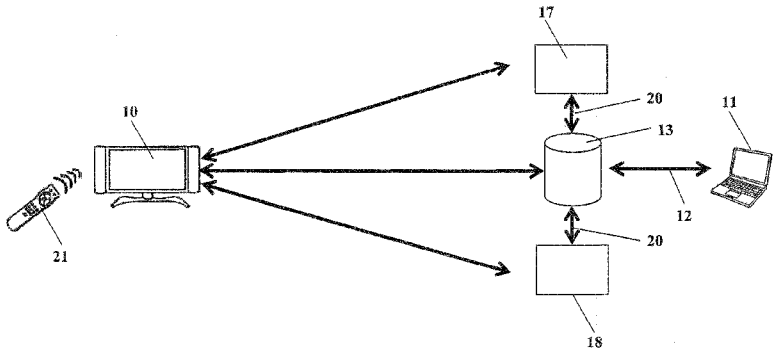

Fig. 4

(57) **Abstract**: The invention relates to a method and an apparatus for authenticating users of a hybrid terminal (10), comprising the generation of a unique registration code (15) and a profile file (19), at least one registration step comprising the inputting of user identification data (14), the inputting and transmission of a personal identification number (16) from the Internet-enabled terminal (11) to a registration server, the transmission of the user identification data (14) relating to the user from the Internet-enabled terminal (11) to the registration server, the inputting of the unique registration code (15), the validation of the user identification data (14) and, if the user identification data (14) correspond to a user reference data record, the assignment to the profile file (19), and, if the personal identification number (16) has not been input by the user, the generation and transmission of the personal identification number (16) from the registration server to the user, and an authentication step comprising a check in order to determine whether the profile file (19) is present in the hybrid terminal (10) and, if so, the carrying out of authentication, otherwise the carrying out of initial authentication, and, if initial authentication reveals that the user is authorized, the generation and transmission of the profile file (19) from the authentication server to the hybrid terminal (10), and, after the initial authentication or authentication has been carried out, the transmission of an enable message to at least one of the service providers (17, 18).

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2012/171568 A1

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

— *Erfindererklärung (Regel 4.17 Ziffer iv)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Die Erfindung betriff ein Verfahren und eine Vorrichtung zur Authentfizierung von Benutzern eines Hybridendgerätes (10), umfassend Generieren eines unikalen Registrierungscodes (15), und einer Profildatei (19), zumindest einen Registrierungsschritt, umfassend Eingeben von Benutzeridentifikationsdaten (14), Eingeben und Übermitteln einer persönlichen Identifikationsnummer (16) von dem internetfähigen Endgerät (11) an einen Registrierungsserver, Übermitteln der Benutzeridentifikationsdaten (14) des Benutzers von dem internetfähigen Endgerät (11) an den Registrierungsserver, Eingeben des unikalen Registrierungscodes (15), Validieren der Benutzeridentifikationsdaten (14) und in dem Fall, dass die Benutzeridentifikationsdaten (14) einem Benutzerreferenzdatensatz entsprechen, Zuordnen der Profildatei (19) und falls das Eingeben der persönlichen Identifikationsnummer (16) durch den Benutzer nicht erfolgt ist, Generieren und Übermitteln der persönlichen Identifikationsnummer (16) von dem Registrierungsserver an den Benutzer, und einen Authentifizierungsschritt, umfassend Prüfen, ob die Profildatei (19) auf dem Hybridendgerät (10) vorhanden ist und falls diese vorhandne ist, Durchführen einer Authentifizierung andernfalls Durchführen einer Erstauthentifizierung und falls die Erstauthentifizierung ergibt, dass der Benutzer berechtigt ist. Generieren und Übertragender Profildatei (19) von dem Authentifizierungsserver an das Hybridendgerät (10), sowie nach Durchfuhren der Erstauthentifizierung oder der Authentifizierung. Übertragen einer Freigabenachricht an zumindest einen der Dienstanbieter (17, 18).

Verfahren und Vorrichtung zur Authentifizierung von Benutzern eines Hybridendgerätes

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Authentifizierung von Benutzern eines Hybridendgerätes.

Derartige Verfahren kommen zur Registrierung und Authentisierung eines Benutzers von Fernsehgeräten und Satellitenempfängern zum Einsatz, die neben dem eigentlichen Empfangsteil für Fernsehprogramme über eine zusätzliche Internetschnittstelle verfügen.

Bekannt sind Verfahren und Vorrichtungen zur Authentifizierung von Fernsehgerätebenutzern.

Aus der Druckschrift DE 10 2006 045 352 A1 geht ein Single-Sign-On-Verfahren für die Nutzung einer Set-Top-Box mit einer Internet- und einer Breitbandschnittstelle hervor. Mittels einer von einem Anbieter zu Verfügung gestellten Anmelde- und Authentifizierungsfunktion erfolgt eine Benutzerauthentifizierung nach dem Einschalten einer Set-Top-Box. Verläuft die Authentifizierung des Benutzers erfolgreich, sendet der Anbieter eine Authentifizierungsinformation an die Set-Top-Box. Diese Authentifizierungsinformation wird anschließend für die Registrierung bei einem Dienstanbieter bzw. mehreren Dienstanbietern verwendet. Die Anmelde- und Authentifizierungsfunktion wird nach dem Einschalten der Set-Top-Box aufgerufen und sofern die Authentifizierung erfolgreich ist, eine Authentifizierungsinformation an die Set-Top-Box gesendet. Diese Authentifizierungsinformation wird wiederum mittels der Set-Top-Box an einen Dienstanbieter gesendet und die Set-Top-Box auf diese Weise bei diesem Dienstanbieter registriert. Anschließend erfolgt ein Abgleich zwischen dem Dienstanbieter und dem Anbieter der Anmelde- und Authentifizierungsfunktion zwecks Verifikation der Authentifizierungsinformationen und ggf. die Übermittelung einer entsprechenden Bestätigung vom Anbieter der Authentifizierungsfunktion an den Dienstanbieter.

Die Druckschrift US 2008 / 0141296 A1 zeigt ein Verfahren zum Zugriff auf einen Authentifizierungsserver für ein digitales Mietfernsehsystem. Sobald das Fernsehgerät, das sowohl über eine Internetanbindung als auch einen digitalen TV-Empfänger verfügt, eingeschaltet wird, kontaktiert dieses einen Authentifizierungsserver, um zu bestimmen, ob der Benutzer ein Teilnehmer des Mitservice ist. Erst nach einer Freigabe durch den Serviceprovider mittels des Authentifizierungsservers kann der Benutzer auf das Digitalfernsehangebot zugreifen.

Ein weiteres Verfahren ist beispielsweise der Druckschrift US 2008 / 0127254 A1 zu entnehmen. Um festzustellen, ob der Benutzer eines Fernsehgerätes dem Fernsehgerät bekannt ist, d.h. ob Identifikationsdaten des Benutzers in dem Fernsehgerät vorhanden sind, werden Daten zur Identifikation des Benutzers von einer drahtlosen Kommunikationseinrichtung, die sich in Sichtweite des Fernsehgerätes befindet, zum Fernsehgerät übertragen. Dabei sind die zur Identifikation des Benutzers erforderlichen Daten bereits auf der Kommunikationseinrichtung vorhanden bzw. abgespeichert. Die empfangenen Daten werden in dem Fernsehgerät mit gespeicherten Nutzerprofilen abgeglichen, um das Fernsehgerät anschließend entsprechend zu steuern.

Das Verfahren weist den Nachteil auf, dass die für die Identifikation und Authentifizierung eines Benutzers erforderlichen Daten auf der drahtlosen Kommunikationseinrichtung gespeichert sind, so dass eine Authentifizierung des Benutzers immer nur mittels der zugehörigen Kommunikationseinrichtung erfolgen kann. Dies ist in der Handhabung umständlich und aufwendig. Wird die drahtlose Kommunikationsvorrichtung von Dritten verwendet, wird nicht der wahre Benutzer identifiziert und autorisiert, sondern derjenige Benutzer, dessen Identifikationsdaten auf der drahtlosen Kommunikationseinrichtung gespeichert sind.

Die Aufgabe der vorliegenden Erfindung besteht daher darin, ein sicheres Verfahren vorzuschlagen, das die Handhabung der Authentifizierung vereinfacht. Des Weiteren ist es Aufgabe der Erfindung, eine entsprechende Vorrichtung zur Durchführung des Verfahrens anzugeben.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst. Das erfindungsgemäße Verfahren bietet den Vorteil, dass die Authentifizierung von Benutzern

eines Hybridendgerätes mittels eines dem jeweiligen Benutzer zugeordneten unikalen Registrierungscodes sowie einer persönlichen Identifikationsnummer erfolgt. Ein besonderer Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass der Benutzer einen Authentifizierungsvorgang unmittelbar an dem Hybridendgerät initiieren kann. Möchte der Benutzer auf Dienste und/oder Inhalte zugreifen, die eine vorherige Authentifizierung erfordern, kann der Benutzer direkt über das Hybridendgerät einen unikalen Registrierungscode anfordern und beziehen, ohne sich beispielsweise zunächst über einen internetfähigen Computer registrieren zu müssen. Ferner bietet das erfindungsgemäße Verfahren den Vorteil, dass seitens des Benutzers des Hybridendgerätes nur eine einmalige Anmeldung - im Folgenden als „Single-Sign-on" bezeichnet - erforderlich ist, um sich gegenüber einem der Dienstanbieter oder gegenüber mehreren der Dienstanbietern zu identifizieren. Nach erfolgreicher Authentifizierung des Benutzers kann dieser nicht nur auf die Nutzdaten bzw. Inhalte eines der Dienstanbieter zugreifen, sondern ist grundsätzlich auch für die Übermittelung von Nutzdaten bzw. den Zugriff auf Inhalte weiterer Dienstanbieter legitimiert.

Gemäß einer bevorzugten Weiterbildung des Verfahrens umfasst das Generieren des unikalen Registrierungscodes folgende Schritte: Senden einer Anforderungsnachricht von dem Hybridendgerät an den Registrierungsserver der Authentifizierungsvorrichtung zum Anfordern des unikalen Registrierungscodes, Generieren des angeforderten Registrierungscodes mittels des Registrierungsservers der Authentifizierungsvorrichtung und Übermitteln des unikalen Registrierungscodes von dem Registrierungsserver der Authentifizierungsvorrichtung an das Hybridendgerät. Dies bietet den Vorteil, dass der Registrierungscode unabhängig vom jeweiligen Hybridendgerät erzeugt wird, indem der Benutzer am Hybridendgerät die Erzeugung des Registrierungscodes, beispielsweise durch Drücken einer Taste, veranlasst. Das Hybridendgerät sendet darauf hin eine Anforderungsnachricht an den Registrierungsserver der Authentifizierungsvorrichtung, um dieser zu signalisieren, dass ein unikaler Registrierungscode erzeugt werden soll. Daraufhin wird mittels des Registrierungsservers der Authentifizierungsvorrichtung der jeweilige unikale Registrierungscode erzeugt. Der unikale Registrierungscode ist eindeutig und unverwechselbar, d.h. die Erzeugung zweier identischer Codes wird in jedem Fall vermieden. Anschließend wird der erzeugte unikale Registrierungscode von dem Registrierungsserver der Authentifizierungsvorrichtung an das Hybridendgerät übermittelt.

Eine weitere bevorzugte Weiterbildung des Verfahrens zeichnet sich dadurch aus, dass das Generieren des unikalen Registrierungscodes mittels des Hybridendgeräts erfolgt. Dies bietet den Vorteil, dass der Registrierungscode lokal mittels des Hybridendgerät erzeugt werden kann, ohne dass dieser zunächst von dem Registrierungsserver der Authentifizierungsvorrichtung an das Hybridendgerät übermittelt werden muss.

Eine zweckmäßige Ausgestaltung der Erfindung ist dadurch gekennzeichnet, dass das Durchführen der Erstauthentifizierung umfasst: Eingeben des unikalen Registrierungscodes und der persönlichen Identifikationsnummer mittels des Hybridendgerätes, Übermitteln des unikalen Registrierungscodes und der persönlichen Identifikationsnummer an einen Authentifizierungsserver der Authentifizierungsvorrichtung über die Internetschnittstelle des Hybridendgerätes, Prüfen des unikalen Registrierungscodes und der persönlichen Identifikationsnummer in dem Authentifizierungsserver der Authentifizierungsvorrichtung durch Abgleich des unikalen Registrierungscodes und der persönlichen Identifikationsnummer mit den Benutzeridentifikationsdaten der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung gespeichert sind, und falls das Prüfen ergibt, dass der unikale Registrierungscode und die persönliche Identifikationsnummer einem der Benutzer zuordenbar sind, Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter und/oder zum Senden der Nutzdaten an den Dienstanbieter berechtigt ist. Greift der Benutzer erstmalig auf die Nutzdaten eines der Dienstanbieter zu, muss dieser sich zunächst mittels der Erstauthentifizierung für den Zugriff auf die Nutzdaten des Dienstanbieters legitimieren. Die Legitimation, ob der Benutzer zum Abruf der Nutzdaten von dem Dienstanbieter berechtigt ist, erfolgt durch Eingabe des unikalen Registrierungscodes und der persönlichen Identifikationsnummer. Die Erstauthentifizierung ist damit in Form einer Zwei-Faktor-Authentifizierung eingerichtet und stellt folglich ein besonders sicheres Verfahren zur Erstauthentifizierung des Benutzers dar.

Eine bevorzugte Weiterbildung der Erfindung zeichnet sich dadurch aus, dass das Durchführen der Authentifizierung umfasst: Übertragen der Profildatei, die auf dem Hybridendgerät abgelegt ist an den Authentifizierungsserver der Authentifizierungsvorrichtung über die Internetschnittstelle des Hybridendgerätes, Prüfen der Profildatei in dem Authentifizierungsserver der Authentifizierungsvorrichtung durch Abgleich der

Profildatei mit den Benutzeridentifikationsdaten der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung gespeichert sind, und falls das Prüfen ergibt, dass die Profildatei einem der Benutzer zuordenbar ist, Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter und/oder zum Senden der Nutzdaten an den Dienstanbieter berechtigt ist. Dies bietet den Vorteil, dass bei wiederholtem Zugriff des Benutzers auf einen der Dienstanbieter bzw. dessen Nutzdaten keine weitere Eingabe seitens des Benutzers zur Authentifizierung mehr erforderlich ist. Die Legitimation des Benutzers gegenüber dem Dienstanbieter erfolgt durch Übertragen und Prüfen der Profildatei. Dieser Vorgang spielt sich für den Benutzer während des Zugriffs auf die Nutzdaten des Dienstanbieters im Verborgenen ab. So ist es auch möglich auf die Nutzdaten anderer Dienstanbieter zuzugreifen, ohne jedes Mal den Benutzer dazu aufzufordern, sich aktiv zu authentifizieren.

Gemäß einer weiter bevorzugten Ausbildung der Erfindung umfasst das Durchführen der Authentifizierung: Eingeben der persönlichen Identifikationsnummer mittels des Hybridendgerätes, Übertragen der Profildatei, die auf dem Hybridendgerät abgelegt ist, und der persönlichen Identifikationsnummer an den Authentifizierungsserver der Authentifizierungsvorrichtung über die Internetschnittstelle des Hybridendgerätes, Prüfen der persönlichen Identifikationsnummer und der Profildatei in dem Authentifizierungsserver der Authentifizierungsvorrichtung durch Abgleich der persönlichen Identifikationsnummer und der Profildatei mit den Benutzeridentifikationsdaten der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung gespeichert sind, und falls das Prüfen ergibt, dass die persönliche Identifikationsnummer und die Profildatei einem der Benutzer zuordenbar ist, Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter und/oder zum Senden der Nutzdaten an dem Dienstanbieter berechtigt ist. Die zusätzliche Eingabe der persönlichen Identifikationsnummer bietet den Vorteil einer erhöhten Sicherheit der Authentifizierung des Benutzers. Greift der Benutzer beispielsweise auf kostenpflichtige Inhalte zu oder auf Inhalte, die zur Kaufabwicklung dienen, wird der Benutzer einerseits durch die Aufforderung zur Eingabe der persönlichen Identifikationsnummer darauf hingewiesen, dass ihm im Folgenden möglicherweise weitere Kosten entstehen. Andererseits wird sichergestellt, dass der Benutzer nicht unbeabsichtigt auf diese speziellen Inhalte zugreift oder unbeabsichtigt Käufe durchführt.

Eine weitere zweckmäßige Ausbildung der Erfindung ist dadurch gekennzeichnet, dass die Kommunikation zwischen dem internetfähigen Endgerät und der Authentifizierungsvorrichtung über eine sichere Internetnetverbindung mittels eines sicheren Hypertext-Übetragungsprotokolls erfolgt. Auf diese Weise wird die Kommunikation zwischen dem internetfähigen Endgerät und der Authentifizierungsvorrichtung gegen unerwünschtes Abhören und Ausspionieren durch Dritte wirksam geschützt.

Gemäß einer weiteren bevorzugten Ausführungsform umfasst der unikale Registrierungscode ausschließlich numerische Zeichen. So ist der Zeichenvorrat für die Eingabe des Registrierungscodes durch den Benutzer lediglich auf die Ziffern 0, 1, 2, 3, 4, 5, 6, 7, 8 und 9 beschränkt, so dass die Eingabe des unikalen Registrierungscodes aufgrund des beschränkten Zeichenvorrats wesentlich erleichtert wird. In einer besonders bevorzugten Ausführungsform erfolgt das Eingeben des unikalen Registrierungscodes und der persönlichen Identifikationsnummer mittels einer Fernbedienung des Hybridendgerätes. Der unikale Registrierungscode und die persönlichen Identifikationsnummer können daher bequem über die Zifferntasten der Fernbedienung eingegeben werden.

Eine weitere zweckmäßige Ausgestaltung der Erfindung ist dadurch gekennzeichnet, dass die Nutzdaten zumindest im Wesentlichen Videodaten und/oder Audiodaten umfassen. Wie zuvor bereits beschrieben, umfassen die Nutzdaten darüber hinaus weitere Steuerdaten, nämlich neben den eigentlichen Audio- und Videodaten zusätzliche Daten, die eine Verknüpfung der übertragenen Audio- und Videodaten mit Inhalten des Internets gewährleisten. Gemäß einer weiteren Ausbildung umfassen die Nutzdaten Kommunikations- und Freigabedaten, die beispielsweise zur Kaufabwicklung dienen. Greift der Benutzer auf Inhalte von Dienstanbietern zu, die einen Onlineshop zum Kauf von Artikeln oder Dienstleistungen bereitstellen, erfolgt die Kaufabwicklung durch die Übermittelung entsprechender Kommunikations- und Freigabedaten über die Breitbandschnittstelle.

Die Aufgabe wird auch durch eine Vorrichtung mit den Merkmalen des Anspruchs 13 gelöst. Die sich daraus ergebenden Vorteile wurden bereits im Zusammenhang mit dem Verfahren beschreiben. Zur Vermeidung von Wiederholungen wird deshalb auf die entsprechenden Passagen der Beschreibung verwiesen.

Sowohl für das erfindungsgemäße Verfahren als auch für die erfindungsgemäße Vorrichtung kann es vorteilhaft sein, dass das Hybridendgerät als HbbTV-Hybridendgerät („Hybrid Broadcast Broadband TV") ausgebildet, das in dem Entwurf zur technischen Spezifikation TS 102 796 V1.1.1 (2009-12) - im Folgenden kurz als HbbTV-Standard bezeichnet - des European Telecommunications Standards Institute 2009 näher definiert ist. Gemäß des HbbTV-Standards wird eine Plattform für die Signalisierung, den Transport und die Präsentation erweiterter und interaktiver Anwendungen zum Betrieb auf Hybridendgeräten festgelegt, die sowohl über eine Breitbandschnittstelle als auch über eine Internetschnittstelle verfügen. Bei derartigen Hybridendgeräten handelt es sich bevorzugt um Fernsehgeräte, Satellitenempfänger, Kabelfernsehempfänger, Settop-Boxen oder dergleichen. Das Hybridendgerät kommuniziert daher sowohl über die Internetschnittstelle als auch über die Breitbandschnittstelle. Ist das Hybridendgerät beispielsweise als erweitertes Fernsehgerät oder Set-Top-Box ausgebildet, empfängt das Hybridendgerät über die Breitbandschnittstelle neben den Nutzdaten in Form von Audio- und Videodaten zusätzliche Informationen, beispielsweise in Form einer eingebetteten Internetadresse, die eine Verknüpfung des Fernsehsignals mit Informationen und Mehrwertangeboten, die über das Internet abrufbar sind, erlauben. Mittels dieser zusätzlichen Informationen, ist es möglich, über die Interschnittstelle des Hybridendgerätes mit dem Internet zu kommunizieren und gezielt auf Inhalte im Internet zuzugreifen, die so mit den über die Breitbandschnittstelle übertragenen Nutzdaten verknüpft sind. Die Übertragung der Nutzdaten erfolgt bevorzugt unidirektional, beispielsweise ausgehend von einem Fernsehsender zu dem Hybridendgerät. Die Breitbandstelle ist daher bevorzugt als DVB-S-, DVB-S2-, DVB-T- bzw. DVB-C-Schnittstelle ausgebildet. Jedoch ist die Breitbandschnittstelle nicht ausschließlich auf den Empfang von Fernsehsignalen gemäß der vorgenannten DVB-Standards beschränkt, sondern grundsätzlich auch zum Empfang von Fernsehsignalen gemäß anderer üblicher Fernsehsignal-Übertragungsverfahren angepasst und eingerichtet.

Weitere bevorzugte oder zweckmäßige Merkmale und Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen und der Beschreibung. Besonders bevorzugte Ausführungsformen werden anhand der beigefügten Zeichnung näher erläutert. Die Zeichnung zeigt:

Fig. 1 schematisch den Ablauf eines ersten Registrierungsschritts,

Fig. 2 schematisch das Durchführen einer Erstauthentifizierung,

Fig. 3 schematisch das Durchführen einer Authentifizierung, und

Fig. 4 eine Prinzipdarstellung der erfindungsgemäßen Vorrichtung.

Dem in der Figur 1 gezeigten Ablauf des ersten Registrierungsschritts gehen folgende, in der Figur 1 nicht gezeigte, Schritte voraus. Zunächst werden ein jeweils unikaler Registrierungscode 15 sowie eine Profildatei 19 generiert, und die Profildatei 19 dem jeweiligen Registrierungscode 15 zugeordnet. Der unikale Registrierungscode 15 ist eindeutig ausgebildet, so dass bei jedem Generieren eines der unikalen Registrierungscodes 15 ein jeweils anderer unikaler Registrierungscode 15 erzeugt wird. Die dem unikalen Registrierungscode 15 zugeordnete Profildatei 19 wird anschließend auf dem Hybridendgerät 10 abgelegt, d.h. auf dem Hybridendgerät 10 bzw. einer dem Hybridendgerät 10 zugeordneten Speichereinrichtung gespeichert. Der unikale Registrierungscode 15 wird über das Hybridendgerät 10 ausgegeben, so dass dieser dem Benutzer angezeigt wird. Vorzugsweise notiert sich der Benutzer den angezeigten unikalen Registrierungscode 15 für die weitere Verwendung. Die Ausgabe des unikalen Registrierungscode 15 kann beispielsweise über einen an das Hybridendgerät 10 angeschlossenen Bildschirm erfolgen. Alternativ erfolgt die Anzeige des Registrierungscode 15 direkt am Hybridendgerät 10, beispielsweise über ein separates Display.

Gemäß des in der Figur 1 gezeigten ersten Registrierungsschritts gibt der Benutzer des Hybridendgerätes 10 anschließend seine Benutzeridentifikationsdaten 14 mittels eines internetfähigen Endgerätes 11 ein. Zur Eingabe der Benutzeridentifikationsdaten 14 ist jedes übliche internetfähige Endgerät geeignet, beispielsweise ein Laptop, ein Desktopcomputer, ein PDA, ein internetfähiges Mobiltelefon oder dergleichen. Die Eingabe der Benutzeridentifikationsdaten 14, bei denen es sich beispielsweise um personenbezogenen Daten wie Name, Anschrift, Bankverbindung bzw. Kreditkartendaten des Benutzers handelt, werden von dem internetfähigen Endgerät 11 über eine erste Internetverbindung 12 an einen Registrierungsserver einer Authentifizierungsvorrichtung 13 übermittelt. Um sicherzustellen, dass die erste Internetverbindung 12 abhörsicher und

gegen Eingriffe von Außen gesichert ist, erfolgt die Kommunikation zwischen dem internetfähigen Endgerät 11 und der Authentifizierungsvorrichtung 13 vorteilhafter Weise über eine gesicherte Internetverbindung mittels eines sicheren Hypertext-Übertragungsprotokolls (HTTPS-Protokoll). Alternativ kann die Kommunikation zwischen dem internetfähigen Endgerät 11 und der Authentifizierungsvorrichtung 13 auch ungesichert oder aber mittels anderer Verschlüsselungsverfahren erfolgen.

Ferner wird der Benutzer zur Eingabe einer persönlichen Identifikationsnummer 16 aufgefordert. Die persönliche Identifikationsnummer 16 ist von dem Benutzer frei wählbar, d.h. der Benutzer kann die persönliche Identifikationsnummer 16 nach seinem Belieben festlegen. Das Eingeben der persönlichen Identifikationsnummer 16 erfolgt ebenfalls mittels des internetfähigen Endgerätes 11. Hierbei hat der Benutzer die Wahl, ob er die persönliche Identifikationsnummer 16 selbst wählen möchte. Folgt der Benutzer der Aufforderung zum Eingeben der persönlichen Identifikationsnummer 16, wird die persönliche Identifikationsnummer 16 nach dem Eingeben von dem internetfähigen Endgerät 11 an den Registrierungsserver der Authentifizierungsvorrichtung 13 über die erste Internetverbindung übermittelt. Folgt der Benutzer der Aufforderung zum Eingeben der persönlichen Identifikationsnummer 16 hingegen nicht, wird die persönliche Identifikationsnummer 16 in einem weiter unten beschriebenen Schritt generiert. Anders ausgedrückt, wird in dem Fall, dass der Benutzer die persönliche Identifikationsnummer 16 selbst festlegt und mittels des internetfähigen Endgerätes 11 eingibt, die persönliche Identifikationsnummer 16 ebenso wie die Benutzeridentifikationsdaten 14 von dem internetfähigen Endgerät 11 über eine erste Internetverbindung 12 an den Registrierungsserver der Authentifizierungsvorrichtung 13 übermittelt. Gibt der Benutzer keine persönliche Identifikationsnummer 16 ein, erfolgt nur die Übermittelung der Benutzeridentifikationsdaten 14. Die persönliche Identifikationsnummer 16 wird in der Authentifizierungsvorrichtung 13 erst anschließend generiert.

Nach Übermitteln der Benutzeridentifikationsdaten 14 des Benutzers von dem internetfähigen Endgerät 11 an den Registrierungsserver der Authentifizierungsvorrichtung 13 über die erste Internetverbindung 12 wird der Benutzer zum Eingeben des unikalen Registrierungscodes 15 mittels des internetfähigen Endgeräts 11 aufgefordert. Der eingegebene unikale Registrierungscode 15 wird anschließend von dem

internetfähigen Endgerät 11 an den Registrierungsserver der Authentifizierungsvorrichtung 13 übermittelt.

Die Benutzeridentifikationsdaten 14 werden anschließend validiert, indem die Benutzeridentifikationsdaten 14 mit einem vorgegebenen Benutzerreferenzdatensatz verglichen werden. Der Benutzerreferenzdatensatz umfasst Informationen, die zur Überprüfung der Identität des Benutzers anhand der auf dem Registrierungsserver vorliegenden Benutzeridentifikationsdaten 14 geeignet sind. Mit anderen Worten ist der Benutzerreferenzdatensatz an die zu überprüfenden Benutzeridentifikationsdaten 14 angepasst. Beispielsweise umfasst dieser zur Überprüfung von Kontodaten Informationen zur Kreditwürdigkeit des Benutzers bzw. zur Überprüfung der Kreditkartendaten entsprechende Kontrolldaten, die zur Feststellung, ob die vorliegenden Benutzeridentifikationsdaten 14 einer gültigen Kreditkarte entsprechen erforderlich sind. Selbstverständlich kann der Benutzerreferenzdatensatz auch der Altersverifikation oder schlicht der Feststellung der tatsächlichen Identität des Benutzers dienen.

In dem Fall, dass die Benutzeridentifikationsdaten 14 einem der vorgegebenen Benutzerreferenzdatensätzen entsprechen, werden die Benutzeridentifikationsdaten 14 des Benutzers auf einem Speichermedium der Authentifizierungsvorrichtung 13 gespeichert. Die Benutzeridentifikationsdaten 14 sind damit dauerhaft gesichert und jederzeit in der Authentifizierungsvorrichtung 13 abrufbar. Als Speichermedium finden sämtliche üblichen bekannten Speichertechnologien Anwendung. Ferner wird die Profildatei 19 dem jeweiligen Benutzer zugeordnet. Anderes ausgedrückt wird eine Korrespondenz zwischen der Profildatei 19 und dem Benutzer hergestellt, die die Identifikation des Benutzers über die Profidatei 19 erlaubt.

Falls der Benutzer zuvor keine persönliche Identifikationsnummer 16 eingegeben hat, erfolgt anschließend die Generierung der persönlichen Identifikationsnummer 16. Anhand des unikalen Registrierungscodes 15 und der persönlichen Identifikationsnummer 16 ist der Benutzer eindeutig identifizierbar, d.h. der unikale Registrierungscode 15 und/oder die persönliche Identifikationsnummer 16 sind dem Benutzer zugeordnet. Vorzugsweise umfasst der unikale Registrierungscode 15 einen 16-stelligen numerischen Hash-Wert, der auf Basis der Benutzeridentifikationsdaten 14 erzeugt wird. Die Erzeugung des Hash-Werts erlaubt die spätere Durchführung eines Plausibilitätschecks, um die Korrektheit des

unikalen Registrierungscodes 15 überprüfen zu können. Selbstverständlich ist der unikale Registrierungscode 15 nicht ausschließlich auf 16-stellige numerische Hash-Werte beschränkt, sondern kann jede beliebige Registrierungscodelänge aufweisen.

Die persönliche Identifikationsnummer 16 wird von dem Registrierungsserver an den Benutzer oder an das internetfähige Endgerät 11 auf separatem Weg übermittelt. Beispielsweise wird dem Benutzer die persönliche Identifikationsnummer 16 per Email oder SMS übermittelt. Auch ist es möglich die persönliche Identifikationsnummer 16 nicht elektronisch, sondern auf dem Postweg zu übermitteln. In jedem Fall erfolgt die Übermittelung der persönlichen Identifikationsnummer 16 nicht innerhalb einer Nachricht über die erste Internetverbindung 12. Folglich ist es auch möglich, sowohl die persönliche Identifikationsnummer 16 als auch den unikalen Registrierungscode 15 ausschließlich über die erste Internetverbindung 12 zu übermitteln. Ein derartige Übermittelung erfolgt jedoch zeitlich derart versetzt, dass beim Abhören der ersten Internetverbindung 12 ein unberechtigter Dritter zugleich weder Kenntnis von dem unikalen Registrierungscode 15 als auch der persönlichen Identifikationsnummer 16 erhält. So wird vermieden, dass unberechtigte Dritte weder Kenntnis von dem unikalen Registrierungscode 15 noch von der persönlichen Identifikationsnummer 16 erhalten. Damit ist ein Missbrauch durch unberechtigte Dritte weitestgehend ausgeschlossen.

Sobald der Benutzer auf einen Dienstanbieter 17, 18 zugreifen möchte, der Benutzer also Nutzdaten von einem Dienstanbieter 17, 18 beziehen will oder Dienste eines Dienstanbieters 17, 18 in Anspruch nehmen möchte, wird zunächst festgestellt, ob der Benutzer zum Zugriff auf den Dienstanbieter 17, 18 berechtigt ist. Diese Überprüfung erfolgt in dem weiter unten beschriebenen Authentifizierungsschritt.

Dazu wird überprüft, ob die Profildatei 19 auf dem Hybridendgerät 10 vorhanden ist, wobei das Hybridendgerät 10 über die Internetschnittstelle mit einem Applikationsserver der Authentifizierungsvorrichtung 13 kommuniziert. Versucht der Benutzer auf einen Dienstanbieter 17, 18 zuzugreifen, beginnt der Applikationsserver mit der Prüfung, ob eine dem Benutzer zugeordnete Profildatei 19 auf dem Hybridendgerät vorhanden ist. So wird festgestellt, ob der Benutzer bereits früher auf einen authentisierungspflichtigen Dienstanbieter 17, 18 zugegriffen hat. Die Profildatei 19 ist als Cookie oder als Client-

Server-Zertifikat ausgebildet, so dass anhand der Profildatei 19 der Benutzer eindeutig identifizierbar ist.

In dem Fall, dass auf dem Hybridendgerät 10 die dem Benutzer zugeordnete Profildatei 19 vorhanden ist, erfolgt die Durchführung einer Authentifizierung, um festzustellen, ob der Benutzer zum Empfangen von Nutzdaten von dem Dienstanbieter 17, 18 berechtigt ist. Die Berechtigung des Benutzers setzt voraus, dass sich dieser in dem Registrierungsschritt identifiziert und dem Benutzer ein zur eindeutigen Identifikation generierter Registrierungscode 15 sowie eine persönliche Identifikationsnummer 16 zugeordnet worden ist. Ist auf dem Hybridendgerät 10 keine dem Benutzer zugeordnete Profildatei 19 vorhanden, erfolgt die Durchführung der Erstauthentifizierung, um festzustellen, ob der Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter 17, 18 und/oder zum Senden der Nutzdaten an den Dienstanbieter 17, 18 berechtigt ist. Ergibt die Erstauthentifizierung, dass der Benutzer berechtigt ist, d.h. zum Empfangen der Nutzdaten von dem Dienstanbieter 17, 18 und/oder zum Senden der Nutzdaten an den Dienstanbieter legitimiert ist, wird die dem Benutzer zugeordnete Profildatei 19 generiert. Die Profildatei 19 wird von dem Authentifizierungsserver der Authentifizierungsvorrichtung 13 auf das Hybridendgerät 10 übertragen und auf dem Hybridendgerät 10 ablegt, d.h. dauerhaft auf dem Hybridendgerät 10 gespeichert. Die Profildatei 19 bleibt auch über einen Neustart des Hybridendgerätes 10 und über längere stromlose Phasen erhalten. Anders ausgedrückt wird durch das Vorhandensein bzw. das Nichtvorhandensein der Profildatei 19 auf dem Hybridendgerät 10 erkannt, ob der Benutzer als ein berechtigter Benutzer bereits vormals auf einen Dienstanbieter 17, 18 zugegriffen hat oder ob es sich um den ersten Zugriff auf einen der Dienstanbieter 17, 18 handelt.

Nach durchgeführter Authentifizierung bzw. Erstauthentifizierung und Feststellung, dass es sich bei dem Benutzer um einen berechtigten Benutzer handelt, wird eine Freigabenachricht an einen oder mehrere Dienstanbieter 17, 18 übertragen. Mittels der Freigabenachricht wird dem Dienstanbieter 17, 18 signalisiert, dass der Benutzer sich als berechtigter Benutzer für den Zugriff auf die Dienste des Dienstanbieters 17, 18 authentifiziert hat. Die Freigabenachricht wird dabei über die zweite Internetverbindung 20 von der Authentifizierungsvorrichtung 13 an die Dienstanbieter 17, 18 übertragen. Im Gegenzug werden die Nutzdaten von dem Dienstanbieter 17, 18 über die Breitbandschnittstelle an das Hybridendgerät 10 übermittelt. Die Übermittelung von Nutzdaten ist dabei nicht

nur auf eine Übermittlung von Nutzdaten von dem Dienstanbieter 17, 18 zu dem Hybridgerät 10 beschränkt. Alternativ umfasst das Übermitteln auch die Übertragung von Daten bzw. Nutzdaten von dem Hybridendgerät 10 an den Dienstanbieter 17, 18. Dies ist beispielsweise der Fall, wenn der Benutzer über den Dienstanbieter 17, 18 kostenpflichtige Dienste in Anspruch nimmt, z.B. beim Erwerb von Waren über den Dienstanbieter 17, 18.

Gemäß einer bevorzugten Weiterbildung der Erfindung erfolgt das Generieren des unikalen Registrierungscodes 15 mittels des Registrierungsservers der Authentifizierungsvorrichtung 13. Initiiert wird dieser Vorgang durch das Senden einer Anforderungsnachricht von dem Hybridendgerät 10 an den Registrierungsserver der Authentifizierungsvorrichtung 13, beispielsweise durch Auswählen eines entsprechenden Menüpunktes in der Menüführung des Hybridendgerätes 10. Alternativ kann der Sendevorgang über eine Taste am Hybridendgerät 10 bzw. an dessen Fernbedienung ausgelöst werden. Nach Empfang der Anforderungsnachricht wird mittels des Registrierungsservers der Authentifizierungsvorrichtung 13 der unikale Registrierungscode 15 generiert und im Anschluss von dem Registrierungsserver an das Hybridendgerät 10 übermittelt.

Eine weitere bevorzugte Ausbildung der Erfindung zeichnet sich dadurch aus, dass der unikale Registrierungscode 15 mittels des Hybridendgerätes 10 generiert wird. Mit anderen Worten erfolgt die Generierung des unikalen Registrierungscodes 15 nicht, wie zuvor beschrieben, durch den Registrierungsserver, sondern lokal auf dem Hybridendgerät 10. Der Erzeugung des unikalen Registrierungscodes 15 kann sowohl auf bestimmten Hardwaremerkmalen des Hybridendgerätes 10 basierend erfolgen, als auch unabhängig von diesen Hardwaremerkmalen. Im Fall einer hardwaregebundenen Erzeugung des unikalen Registrierungscodes 15 wird die Registrierungscodeerzeugung an eindeutige Merkmale des Hybridendgerätes 10, beispielsweise an eine eindeutigen Seriennummer des Hybridgerätes 10 oder dergleichen, gebunden. Geeignet ist selbstverständlich auch jedes andere Hardwaremerkmal des Hybridendgeräts 10, das die Generierung des unikalen Registrierungscodes 15 erlaubt. Alternativ erfolgt die Erzeugung des unikalen Registrierungscodes 15 unabhängig von Hardwaremerkmalen des Hybridendgerätes 10. So kann die Registrierungscodeerzeugung beispielsweise mittels beliebiger mathematischer Verfahren erfolgen, sofern dieses sicherstellen, dass der jeweils erzeugte unikale Registrierungscode 15 eindeutig ist.

Eine bevorzugte Weiterbildung der Erfindung ist in Fig. 2 gezeigt, die das Durchführen der Erstauthentifizierung schematisch darstellt. Zur Erstauthentifizierung wird der Benutzer aufgefordert, den unikalen Registrierungscode 15 und die persönliche Identifikationsnummer 16 mittels des Hybridendgerätes 10 einzugeben. Der unikale Registrierungscode 15 sowie die persönliche Identifikationsnummer 16 werden über die Internetschnittstelle des Hybridendgerätes 10 an einen Authentifizierungsserver der Authentifizierungsvorrichtung 13 übermittelt. Der Authentifizierungsserver überprüft den unikalen Registrierungscode 15 in Verbindung mit der persönlichen Identifikationsnummer 16 darauf hin, ob der unikale Registrierungscode 15 und die persönliche Identifikationsnummer 16 einem der Benutzer zuordenbar ist. Dies geschieht durch Abgleich des unikalen Registrierungscodes 15 und der persönlichen Identifikationsnummer 16 mit den Benutzeridentifikationsdaten 14, die auf dem Speichermedium der Authentifizierungsvorrichtung 13 gespeichert sind. Ergibt der Abgleich, dass der unikale Registrierungscode 15 und die persönliche Identifikationsnummer 16 einem der Benutzer zuordenbar ist, wird festgestellt, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter 17, 18 und/oder zum Senden der Nutzdaten an den Dienstanbieter 17, 18 berechtigt ist. Anschließend wird die dem Benutzer zugeordnete Profildatei 19 von dem Authentifizierungsserver der Authentifizierungsvorrichtung 13 über die Internetschnittstelle auf das Hybridendgerät 10 übertragen und auf dem Hybridendgerät 10 abgelegt.

Gemäß einer weiter bevorzugten Ausführungsform der Erfindung, entsprechend der schematisch dargestellten Durchführung einer Authentifizierung in Fig. 3, wird, sofern ein Benutzer auf einen Dienstanbieter 17, 18 zugreifen möchte, die auf dem Hybridendgerät 10 abgelegte Profildatei 19 an den Authentifizierungsserver der Authentifizierungsvorrichtung 13 über die Internetschnittstelle des Hybridendgerätes 10 übertragen. Die Profildatei 19 wird in dem Authentifizierungsserver der Authentifizierungsvorrichtung 13 durch Abgleich der Profildatei 19 mit den Benutzeridentifikationsdaten 14 abgeglichen. Die Benutzeridentifikationsdaten 14 sind auf dem Speichermedium der Authentifizierungsvorrichtung 13 gespeichert. Ergibt der Abgleich bzw. die Prüfung, dass die Profildatei 19 einem der Benutzer zuordenbar ist, ist dieser Benutzer als berechtigter Benutzer erkannt und es wird festgestellt, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter 17, 18 und/oder zum Senden der Nutzdaten an den Dienstanbieter berechtigt ist. Mit anderen Worten wird der Benutzer aufgrund des

Vorhandenseins der Profildatei 19 auf dem Hybridendgerät 10 eindeutig identifiziert und als Berechtiger bzw. autorisierter Benutzer erkannt. Damit ist der Benutzer nach einem einmaligen Zugriff auf einen Dienstanbieter 17, 18 einschließlich erfolgter Authentifizierung über das Vorhandensein der Profildatei 19 eindeutig identifizierbar. Dies bietet den Vorteil, dass der Benutzer für alle Dienstanbieter 17, 18, für den die Profildatei den Benutzer als berechtigten Benutzer ausweist, authentifiziert ist. Greift der Benutzer auf einen weiteren Dienstanbieter 17, 18 zu, um von diesem Nutzdaten zu empfangen oder an diesen Nutzdaten zu senden, erfolgt die Prüfung, ob der Benutzer für diesen Zugriff auf den Dienstanbieter 17, 18 berechtigt ist, über das Vorhandensein der Profildatei 19 auf dem Hybridendgerät 10. Mit anderen Worten genügt die einmalige Authentifizierung durch Eingeben des unikalen Registrierungscodes 15 und der persönlichen Identifikationsnummer 16, um sich bei einer Vielzahl von Dienstanbietern 17, 18 als berechtigter Benutzer zu authentifizieren, ohne bei jedem Zugriff auf einen anderen Dienstanbieter 17, 18 erneut den unikalen Registrierungscode 15 und die persönliche Identifikationsnummer 16 eingeben zu müssen.

Gemäß einer weiter bevorzugten Ausführungsform der Erfindung erfolgt neben der Übermittelung der Profildatei 19 zusätzlich die Eingabe und die anschließende Übermittelung der persönlichen Identifikationsnummer 16. Sollen Nutzdaten von einem der Dienstanbieter 17, 18 empfangen oder an diesen gesendet werden, die eine besondere Sorgfalt hinsichtlich der Identifizierung und Authentifizierung des Benutzer erfordern, beispielsweise beim Zugriff auf weitere kostenpflichtige Inhalte oder den Onlineabschluss von Kaufverträgen, wird der Benutzer aufgefordert, seine persönliche Identifikationsnummer 16 einzugeben. Sowohl die Profildatei 19 als auch die persönliche Identifikationsnummer 16 werden über die Internetschnittstelle des Hybridendgerätes 10 an den Authentifizierungsserver der Authentifizierungsvorrichtung 13 übertragen. Ergibt die Prüfung der persönlichen Identifikationsnummer 16 und der Profildatei 19, dass diese einem der Benutzer zuordenbar ist, erfolgt die Feststellung, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter 17,18 und/oder zum Senden der Nutzdaten an den Dienstanbieter berechtigt ist. Die Berechtigung des Benutzers wird durch Abgleich der persönlichen Identifikationsnummer 16 und der Profildatei 19 mit den entsprechenden Benutzeridentifikationsdaten 14, die auf dem Speichermedium der Authentifizierungsvorrichtung gespeichert sind, geprüft.

Vorzugsweise ist die persönliche Identifikationsnummer 16 von dem Benutzer frei wählbar und umfasst üblicher Weise vier numerische Zeichen. Auf diese Weise ist die Authentifizierung für den Benutzer besonders komfortabel, da nur vier numerische Zeichen einzugeben sind. Alternativ weist die persönliche Identifikationsnummer mehr als vier Zeichen auf und umfasst ferner auch beliebige nicht numerische Zeichen.

Eine weitere Ausführungsform zeichnet sich dadurch aus, dass das Eingeben des unikalen Registrierungscodes 15 und der persönlichen Identifikationsnummer 16 mittels einer Fernbedienung 21 des Hybridgerätes erfolgt. Der Benutzer kann auf diese Weise sehr komfortabel mit der sowieso zur Bedienung des Hybridendgerätes 10 erforderlichen Fernbedienung 21 den unikalen Registrierungscode 15 sowie die persönliche Identifikationsnummer 16 eingeben.

Gemäß einer weiteren bevorzugten Ausführungsform umfassen die Nutzdaten zumindest im Wesentlichen Videodaten und/oder Audiodaten. Typischerweise umfassen die Nutzdaten digitale Fernsehdaten. Die Nutzdaten sind aber nicht ausschließlich auf Fernsehdaten beschränkt, sondern umfassen jegliche Form von Audio- und Videodaten. Ferner umfassen die Nutzdaten Steuerdaten, die für die korrekte Übertragung der Audio- und Videodaten üblicherweise mit übertragen werden.

Zur Verknüpfung der Audio- und Videodaten, d.h. der von den Dienstanbietern 17, 18 übermittelten Inhalte, umfassen die Nutzdaten ferner eingebettete Internetadressen. Damit findet eine Synchronisation zwischen den Nutzdaten, beispielsweise einem laufenden Fernsehprogramm, und gewöhnlichen HTML-Internetseiten statt. Die Nutzdaten umfassen daher Triggerinformationen sowie Internetadressen, die von dem Hybridendgerät 10 ausgewertet werden. Dies erlaubt es dem Benutzer, auf entsprechende Inhalte im Internet zuzugreifen, die den Nutzdaten zeitlich und inhaltlich zugeordnet sind. Auf diese Weise können die Dienstanbieter interaktive Anwendungen und Informationen anbieten, auf die der Benutzer interaktiv zugreifen kann. Entsprechend einer alternativen Ausführungsform umfassen die Nutzdaten Kommunikations- und Freigabedaten, die zur Abwickelung von Onlinegeschäften zwischen dem Benutzer und dem Dienstanbieter 17, 18 über die Breitbandschnittstelle erforderlich sind.

Fig. 4 zeigt eine Prinzipdarstellung der erfindungsgemäßen Vorrichtung. Die Vorrichtung umfasst das Hybridendgerät 10 mit zumindest einer Internetschnittstelle und zumindest einer Breitbandschnittstelle, die Authentifizierungsvorrichtung 13, wobei die Authentifizierungsvorrichtung 13 den Registrierungsserver, den Applikationsserver, den Authentifizierungsserver und zumindest ein Speichermedium umfasst. Alternativ sind der Registrierungs-, Applikationsserver und der Authentifizierungsserver auf einem Server implementiert. Das Hybridendgerät 10 ist über die Internetschnittstelle mit der Authentifizierungsvorrichtung 13 verbunden und über die Breitbandschnittstelle mit zumindest einem Dienstanbieter 17, 18 verbunden. Die Authentifizierungsvorrichtung 13 ist über die zweite Internetverbindung mit zumindest einem der Dienstanbieter 17, 18 verbunden und derart ausgebildet, dass beispielsweise die Freigabenachricht von der Authentifizierungsvorrichtung 13 an den Dienstanbieter 17, 18 übertragen werden kann.

Ferner ist das internetfähige Endgerät 11 über die erste Internetverbindung 12 mit dem Registrierungsserver der Authentifizierungsvorrichtung 13 verbunden. Dabei ist entweder der Registrierungsserver der Authentifizierungsvorrichtung 13 angepasst, zumindest den unikalen Registrierungscode 15 sowie eine diesem zugeordnete Profildatei 19 beim Empfang einer von dem Hybridendgerät 10 gesendeten Anforderungsnachricht zu generieren und den unikalen Registrierungscode 15 von dem Registrierungsserver der Authentifizierungsvorrichtung 13 an das Hybridendgerät 10 zu übermitteln, oder das Hybridendgerät 10 ist angepasst, zumindest den einen unikalen Registrierungscode 15 sowie die dem Registrierungscode 15 zugeordnete Profildatei 19 zu generieren. Mit anderen Worten ist entweder der Registrierungsserver oder das Hybridendgerät 10 zur Erzeugung des unikalen Registrierungscodes 15 angepasst, wie dies bereits zuvor im Zusammenhang mit dem erfindungsgemäßen Verfahren beschrieben ist. Zur Speicherung der Profildatei 19 auf dem Hybridendgerät 10 ist dieses angepasst, die Profildatei 19 auf dem Hybridendgerät 10 abzulegen und den unikalen Registrierungscode 15 auszugeben, um dem Benutzer den unikalen Registrierungscode 15 anzuzeigen.

Der Registrierungsserver ist ferner angepasst, Benutzeridentifkationsdaten und den unikalen Registrierungscode 15, die vom internetfähigen Endgerät 11 an den Registrierungsserver über die erste Internetverbindung 12 übermittelt werden, durch Vergleich von Benutzeridentifikationsdaten 14 mit einem vorgegebenen Benutzerreferenzdatensatz zu validieren und in dem Fall, dass die Benutzeridentifikations-

daten 14 dem vorgegebenen Benutzerreferenzdatensatz entsprechen, die Benutzeridentifikationsdaten 14 des Benutzers auf dem Speichermedium zu speichern und die Profildatei 19 dem Benutzer zuzuordnen.

Weiter ist der Registrierungsserver angepasst, die persönlichen Identifikationsnummer 16 zu generieren, wobei die persönliche Identifikationsnummer 16 dem Benutzer zugeordnet ist, die persönlichen Identifikationsnummer 16 von dem Registrierungsserver über eine separate Verbindung an den Benutzer oder an das internetfähige Endgerät 11 zu übermitteln.

Der Registrierungsserver ist ferner derart eingerichtet und angepasst, zu prüfen, ob die Profildatei 19 auf dem Hybridendgerät 10 vorhanden ist, wobei das Hybridendgerät 10 eingerichtet ist, über die Internetschnittstelle mit dem Applikationsserver der Authentifizierungsvorrichtung 13 zu kommunizieren und im dem Fall, dass auf dem Hybridendgerät 10 die dem Benutzer zugeordnete Profildatei 19 vorhanden ist, die Authentifizierung durchzuführen, um festzustellen, ob der Benutzer zum Empfangen von Nutzdaten von dem Dienstanbieter 17, 18 berechtigt ist, andernfalls die Erstauthentifizierung durchzuführen, um festzustellen, ob der Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter 17, 18 und/oder zum Senden der Nutzdaten an den Dienstanbieter 17, 18 berechtigt ist, die Profildatei 19 zu generieren, wobei die Profildatei 19 dem Benutzer zugeordnet ist, die Profildatei 19 von dem Authentifizierungsserver der Authentifizierungsvorrichtung 13 über die Internetschnittstelle auf das Hybridendgerät 10 zu übertragen, wobei die Profildatei 19 auf dem Hybridendgerät 10 abgelegt wird, sowie nach der Erstauthentifizierung oder der Authentifizierung, sofern der Benutzer als ein berechtigter Benutzer authentifiziert wurde, einer Freigabenachricht an zumindest einen der Dienstanbieter 17, 18 zu übertragen und die Nutzdaten von dem Dienstanbieter 17, 18 zu übermitteln, an den die Übertragung der Freigabenachricht erfolgt ist, wobei das Hybridendgerät 10 angepasst ist, zur Übermittelung der Nutzdaten über die Breitbandschnittstelle mit dem Dienstanbieter zu kommunizieren.

Ansprüche

1. Verfahren zur Authentifizierung von Benutzern eines Hybridendgerätes (**10**),

wobei das Hybridendgerät (**10**) über zumindest eine Internetschnittstelle kommuniziert und über zumindest eine Breitbandschnittstelle mit zumindest einem Dienstanbieter (**17, 18**) kommuniziert, umfassend

Generieren zumindest eines jeweils unikalen Registrierungscodes (**15**),

Generieren einer Profildatei (**19**) und zuordnen der Profildatei (**19**) zu dem unikalen Registrierungscode (**15**),

Ablegen der Profildatei (**19**) auf dem Hybridendgerät (**10**),

Ausgeben des unikalen Registrierungscodes (**15**) über das Hybridendgerät (**10**), um den unikalen Registrierungscode (**15**) dem Benutzer anzuzeigen,

und zumindest einen ersten Registrierungsschritt umfassend,

Eingeben von Benutzeridentifikationsdaten (**14**) zumindest eines der Benutzer mittels eines internetfähigen Endgerätes (**11**),

Auffordern des Benutzers zum Eingeben einer persönlichen Identifikationsnummer (**16**) mittels des internetfähigen Endgerätes (**11**), wobei die persönliche Identifikationsnummer (**16**) von dem Benutzer frei wählbar ist,

und falls das Eingeben der persönlichen Identifikationsnummer (**16**) durch den Benutzer erfolgt ist, Übermitteln der persönlichen Identifikationsnummer (**16**) von dem internetfähigen Endgerät (**11**) an einen Registrierungsserver einer Authentifizierungsvorrichtung (**13**) über eine erste Internetverbindung (**12**),

Übermitteln der Benutzeridentifikationsdaten (**14**) des Benutzers von dem internetfähigen Endgerät (**11**) an den Registrierungsserver der Authentifizierungsvorrichtung (**13**) über die erste Internetverbindung (**12**),

Auffordern des Benutzers zum Eingeben des unikalen Registrierungscodes (**15**) mittels des internetfähigen Endgeräts (**11**) und Übermitteln des eingegebenen unikalen Registrierungscodes (**15**) von dem internetfähigen Endgerät (**11**) an den Registrierungsserver der Authentifizierungsvorrichtung (**13**),

Validieren der Benutzeridentifikationsdaten (**14**), die auf dem Registrierungsserver vorliegen, durch Vergleichen der Benutzeridentifikationsdaten (**14**) mit einem vorgegebenen Benutzerreferenzdatensatz und in dem Fall, dass die Benutzeridentifikationsdaten dem vorgegebenen Benutzerreferenzdatensatz entsprechen,

Zuordnen der Profildatei (**19**) zu dem Benutzer,

Speichern der Benutzeridentifikationsdaten (**14**) des Benutzers auf einem Speichermedium der Authentifizierungsvorrichtung (**13**),

und falls das Eingeben der persönlichen Identifikationsnummer (**16**) durch den Benutzer nicht erfolgt ist, Generieren von zumindest der persönlichen Identifikationsnummer (**16**), wobei die persönliche Identifikationsnummer (**16**) dem Benutzer zugeordnet ist,

und

Übermitteln der persönlichen Identifikationsnummer (**16**) von dem Registrierungsserver über eine separate Verbindung an den Benutzer oder an das internetfähige Endgerät (**11**),

und einen Authentifizierungsschritt umfassend,

Prüfen, ob die Profildatei (**19**) auf dem Hybridendgerät (**10**) vorhanden ist, wobei das Hybridendgerät (**10**) über die Internetschnittstelle mit einem Applikationsserver der Authentifizierungsvorrichtung (**13**) kommuniziert und

im dem Fall, dass auf dem Hybridendgerät (**10**) die Profildatei (**19**) vorhanden ist,

a) Durchführen einer Authentifizierung um festzustellen, ob der Benutzer zum Empfangen von Nutzdaten von dem Dienstanbieter (**17, 18**) und/oder zum Senden von Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist,

andernfalls

b) Durchführen einer Erstauthentifizierung, um festzustellen, ob der Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter (**17, 18**) und/oder zum Senden der Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist,

und falls die Erstauthentifizierung ergibt, dass der Benutzer berechtigt ist,

Generieren der Profildatei (**19**), wobei die Profildatei (**19**) dem Benutzer zugeordnet ist,

Übertragen der Profildatei (**19**) von dem Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) über die Internetschnittstelle auf das Hybridendgerät (**10**), wobei die Profildatei (**19**) auf dem Hybridendgerät (**10**) abgelegt wird,

sowie nach Durchführen der Erstauthentifizierung oder Durchführen der Authentifizierung, sofern der Benutzer als ein berechtigter Benutzer authentifiziert wurde,

Übertragen einer Freigabenachricht an zumindest einen der Dienstanbieter (**17, 18**) und

Übermitteln der Nutzdaten von dem Dienstanbieter (**17, 18**), an den die Übertragung der Freigabenachricht erfolgt ist, wobei das Hybridendgerät (**10**) zum Übermitteln der Nutzdaten über die Breitbandschnittstelle mit dem Dienstanbieter (**17, 18**) kommuniziert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Generieren des unikalen Registrierungscodes (**15**) folgende Schritte umfasst:

Senden einer Anforderungsnachricht von dem Hybridendgerät (**10**) an den Registrierungsserver der Authentifizierungsvorrichtung (**13**) zum Anfordern des unikalen Registrierungscodes (**15**),

Generieren des angeforderten unikalen Registrierungscodes (**15**) mittels des Registrierungsservers der Authentifizierungsvorrichtung (**13**) und

Übermitteln des unikalen Registrierungscodes (**15**) von dem Registrierungsserver der Authentifizierungsvorrichtung (**13**) an das Hybridendgerät (**10**).

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Generieren des unikalen Registrierungscode (**15**) folgenden Schritt umfasst:

Generieren des unikalen Registrierungscodes (**15**) mittels des Hybridendgerätes (**10**).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Durchführen der Erstauthentifizierung umfasst:

Eingeben des unikalen Registrierungscodes (**15**) und der persönlichen Identifikationsnummer (**16**) mittels des Hybridendgerätes (**10**),

Übermitteln des unikalen Registrierungscodes (**15**) und der persönlichen Identifikationsnummer (**16**) an einen Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) über die Internetschnittstelle des Hybridendgerätes (**10**),

Prüfen des unikalen Registrierungscodes (**15**) und der persönlichen Identifikationsnummer (**16**) in dem Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) durch Abgleich des unikalen Registrierungscodes (**15**) und der persönlichen Identifikationsnummer (**16**) mit den Benutzeridentifikationsdaten (**14**) der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung (**13**) gespeichert sind, und falls das Prüfen ergibt, dass der unikale Registrierungscode (**15**) und die persönliche Identifikationsnummer (**16**) einem der Benutzer zuordenbar sind,

Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter (**17, 18**) und/oder zum Senden der Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das Durchführen der Authentifizierung umfasst:

Übertragen der Profildatei (**19**), die auf dem Hybridendgerät (**10**) abgelegt ist, an den Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) über die Internetschnittstelle des Hybridendgerätes (**10**),

Prüfen der Profildatei (**19**) in dem Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) durch Abgleich der Profildatei (**19**) mit den Benutzeridentifikationsdaten (**14**) der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung (**13**) gespeichert sind, und falls das Prüfen ergibt, dass die Profildatei (**19**) einem der Benutzer zuordenbar ist,

Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter (**17, 18**) und/oder zum Senden der Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist.

6 Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das Durchführen der Authentifizierung umfasst:

Eingeben der persönlichen Identifikationsnummer (**16**) mittels des Hybridendgerätes (**10**),

Übertragen der Profildatei (**19**), die auf dem Hybridendgerät (**10**) abgelegt ist, und der persönlichen Identifikationsnummer (**19**) an den Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) über die Internetschnittstelle des Hybridendgerätes (**10**),

Prüfen der persönlichen Identifikationsnummer (**16**) und der Profildatei (**19**) in dem Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) durch Abgleich der persönlichen Identifikationsnummer (**16**) und der Profildatei (**19**) mit den Benutzeridentifikationsdaten (**14**) der Benutzer, die auf dem Speichermedium der Authentifizierungsvorrichtung (**13**) gespeichert sind, und falls das Prüfen ergibt, dass die persönliche Identifikationsnummer (**16**) und die Profildatei (**19**) einem der Benutzer zuordenbar ist,

Feststellen, dass dieser Benutzer zum Empfangen der Nutzdaten von dem Dienstanbieter (**17, 18**) und/oder zum Senden der Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Hybridendgerät (**10**) über die Internetschnittstelle und über die Breitbandschnittstelle gemäß des HbbTV-Standards kommuniziert, indem das Hybridendgerät (**10**) als HbbTV-Endgerät ausgebildet ist.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Kommunikation zwischen dem internetfähigen Endgerät (**11**) und der Authentifizierungsvorrichtung (**13**) über eine sichere Internetnetverbindung mittels eines sicheren Hypertext-Übertragungsprotokolls erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass der unikale Registrierungscode (**15**) ausschließlich numerische Zeichen umfasst.

10. Verfahren nach einem der Ansprüche 2 bis 9, dadurch gekennzeichnet, dass das Eingeben des unikalen Registrierungscodes (**15**) und der persönlichen Identifikationsnummer (**16**) mittels einer Fernbedienung (**21**) des Hybridendgerätes (**10**) erfolgt.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass die Nutzdaten zumindest im Wesentlichen Videodaten und/oder Audiodaten umfassen.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Nutzdaten Kommunikations- und Freigabedaten umfassen.

13 Vorrichtung zur Authentifizierung von Benutzern eines Hybridendgerätes (**10**) umfassend,

zumindest ein Hybridendgerät (**10**) mit zumindest einer Internetschnittstelle und zumindest einer Breitbandschnittstelle,

eine Authentifizierungsvorrichtung (**13**), wobei die Authentifizierungsvorrichtung (**13**) einen Registrierungsserver, einen Applikationsserver, einen Authentifizierungsserver und zumindest ein Speichermedium umfasst,

und wobei das Hybridendgerät (**10**) über die Internetschnittstelle mit der Authentifizierungsvorrichtung (**13**) verbunden ist und über die Breitbandschnittstelle mit zumindest einem Dienstanbieter (**17, 18**) verbunden ist,

und wobei die Authentifizierungsvorrichtung (**13**) über eine zweite Internetverbindung (**20**) mit zumindest einem der Dienstanbieter (**17, 18**) verbunden ist,

ein internetfähiges Endgerät (**11**), dass über eine erste Internetverbindung (**12**) mit dem Registrierungsserver der Authentifizierungsvorrichtung (**13**) verbunden ist,

wobei entweder

der Registrierungsserver der Authentifizierungsvorrichtung (**13**) angepasst ist, zumindest einen unikalen Registrierungscode (**15**) sowie eine dem Registrierungscode (**15**) zugeordnete Profildatei (**19**) beim Empfang einer von dem Hybridendgerät (**10**) gesendeten Anforderungsnachricht zu generieren und den unikalen Registrierungscode (**15**) von dem Registrierungsserver der Authentifizierungsvorrichtung (**13**) an das Hybridendgerät (**10**) zu übermitteln

oder das Hybridendgerät (**10**) angepasst ist, zumindest den einen unikalen Registrierungscode (**15**) sowie die dem Registrierungscode (**15**) zugeordnete Profildatei (**19**) zu generieren,

und wobei das Hybridendgerät (**10**) angepasst ist, die Profildatei (**19**) auf dem Hybridendgerät (**10**) abzulegen und den unikalen Registrierungscode (**15**) auszugeben, um den unikalen Registrierungscode (**15**) dem Benutzer anzuzeigen, und

wobei

der Registrierungsserver ferner angepasst ist,

Benutzeridentifkationsdaten (14) und den unikalen Registrierungscode (**15**), die vom internetfähigen Endgerät (**11**) an den Registrierungsserver über die erste Internetverbindung (**12**) übermittelt werden, durch Vergleich der Benutzeridentifikationsdaten (**14**) mit einem vorgegebenen Benutzerreferenzdatensatz zu validieren und in dem Fall, dass die Benutzeridentifikationsdaten (**14**) dem vorgegebenen Benutzerreferenzdatensatz entsprechen,

die Profildatei (**19**) dem Benutzer zuzuordnen,

die Benutzeridentifikationsdaten (**14**) des Benutzers auf dem Speichermedium zu speichern,

zumindest eine persönlichen Identifikationsnummer (**16**) zu generieren, wobei die persönliche Identifikationsnummer (**16**) dem Benutzer zugeordnet ist,

die persönlichen Identifikationsnummer (**16**) von dem Registrierungsserver über eine separate Verbindung an den Benutzer oder an das internetfähige Endgerät (**11**) zu übermitteln,

und zu prüfen, ob die Profildatei (**19**) auf dem Hybridendgerät (**10**) vorhanden ist, wobei das Hybridendgerät (**10**) eingerichtet ist, über die Internetschnittstelle mit einem Applikationsserver der Authentifizierungsvorrichtung (**13**) zu kommunizieren und

im dem Fall, dass auf dem Hybridendgerät (**10**) die Profildatei (**19**) vorhanden ist,

a) eine Authentifizierung durchzuführen, um festzustellen, ob der Benutzer zum Empfangen von Nutzdaten von dem Dienstanbieter (**17, 18**) berechtigt ist,

andernfalls

b) eine Erstauthentifizierung durchzuführen, um festzustellen, ob der Benutzer zum Empfangen der Nutzdaten von der Dienstanbieter (**17, 18**) und/oder zum Senden der Nutzdaten an den Dienstanbieter (**17, 18**) berechtigt ist,

die Profildatei (**19**) zu generieren, wobei die Profildatei (**19**) dem Benutzer zugeordnet ist,

die Profildatei (**19**) von dem Authentifizierungsserver der Authentifizierungsvorrichtung (**13**) über die Internetschnittstelle auf das Hybridendgerät (**10**) zu übertragen, wobei die Profildatei (**19**) auf dem Hybridendgerät (**10**) abgelegt wird,

sowie nach der Erstauthentifizierung oder der Authentifizierung, sofern der Benutzer als ein berechtigter Benutzer authentifiziert wurde,

eine Freigabenachricht an zumindest eine der Dienstanbieter (**17, 18**) zu übertragen und

die Nutzdaten von dem Dienstanbieter (**17, 18**) zu übermitteln, an den die Übertragung der Freigabenachricht erfolgt ist, wobei das Hybridendgerät (**10**) angepasst ist, zur Übermittelung der Nutzdaten über die Breitbandschnittstelle mit dem Dienstanbieter zu kommunizieren.

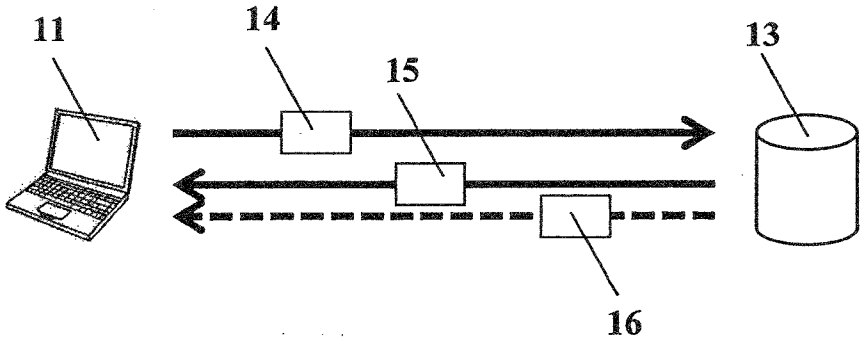

Fig. 1

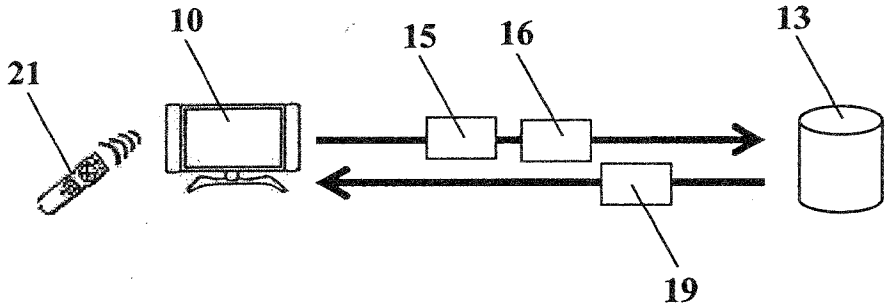

Fig. 2

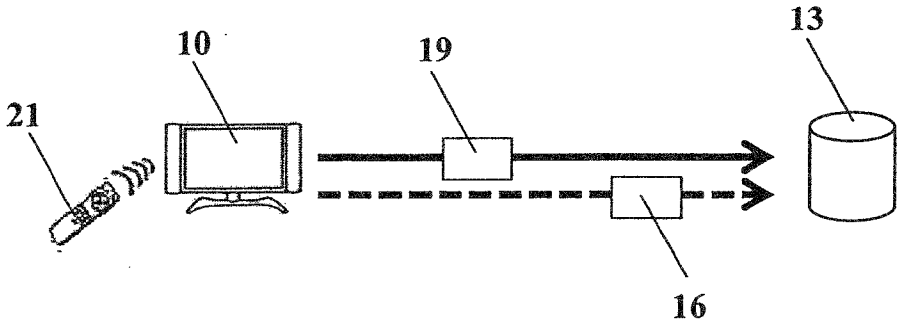

Fig. 3

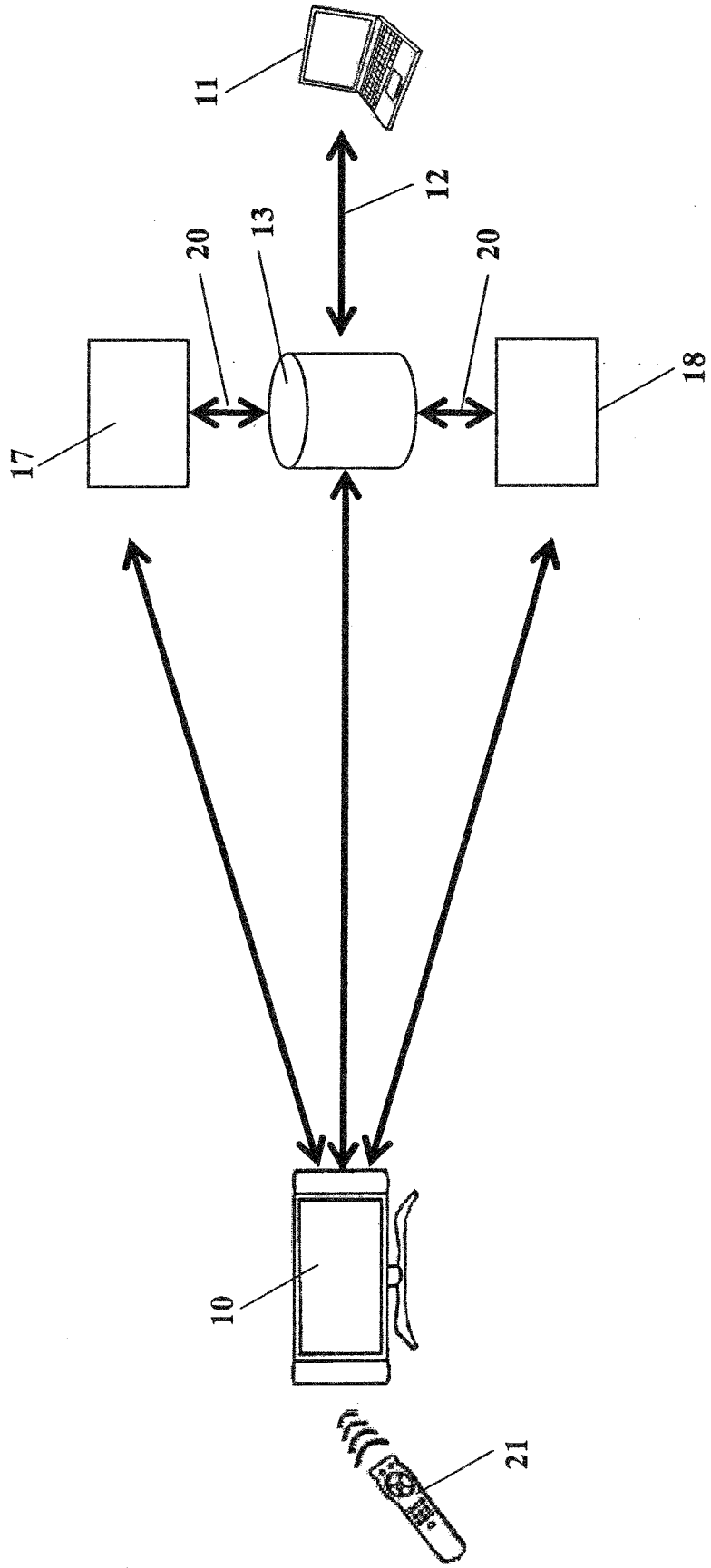

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/060044

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/08 H04N21/258 H04N21/441
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N H04L H04H

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	IGNACIO MÃ Â S ET AL: "IMS-TV: An IMS-based architecture for interactive, personalized IPTV", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 46, no. 11, 1 November 2008 (2008-11-01), pages 156-163, XP011239048, ISSN: 0163-6804, DOI: 10.1109/MCOM.2008.4689259 the whole document -----	1-13
X	US 2010/031290 A1 (HUA SUZANN [US] ET AL) 4 February 2010 (2010-02-04) abstract paragraph [0018] - paragraph [0053] figures 1-5 -----	1-13
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 April 2012	04/05/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dujardin, Corinne

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2006 045352 A1 (NOKIA SIEMENS NETWORKS GMBH [DE]) 10 April 2008 (2008-04-10) cited in the application abstract paragraph [0019] - paragraph [0029] paragraph [0032] - paragraph [0053] figures 1-2	1-13
X	US 2009/220216 A1 (MARSH CHRISTOPHER [US] ET AL) 3 September 2009 (2009-09-03) abstract paragraph [0036] - paragraph [0529] figures 1-24	1-13
X	WO 2008/113827 A2 (VODAFONE ESPANA SA [ES]; VODAFONE PLC [GB]; ALMENAR BELENGUER PEDRO [E) 25 September 2008 (2008-09-25) abstract page 6, line 23 - page 18, line 28 figure 1	1-13
A	"Hybrid Broadcast Broadband TV ; ETSI TS 102 796 V1.1.1" In: "Hybrid Broadcast Broadband TV ; ETSI TS 102 796 V1.1.1", 1 June 2010 (2010-06-01), ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, XP55001426, page 7, line 1 - last line page 11, line 13 - page 56, last line	7

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/060044

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010031290 A1	04-02-2010	NONE	
DE 102006045352 A1	10-04-2008	CN 101518029 A	26-08-2009
		DE 102006045352 A1	10-04-2008
		EP 2084883 A1	05-08-2009
		KR 20090067192 A	24-06-2009
		US 2010023962 A1	28-01-2010
		WO 2008037581 A1	03-04-2008
US 2009220216 A1	03-09-2009	NONE	
WO 2008113827 A2	25-09-2008	ES 2324753 A1	13-08-2009
		WO 2008113827 A2	25-09-2008

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2011/060044

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 H04L29/08 H04N21/258 H04N21/441
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04N H04L H04H

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	IGNACIO MÃ Â S ET AL: "IMS-TV: An IMS-based architecture for interactive, personalized IPTV", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, Bd. 46, Nr. 11, 1. November 2008 (2008-11-01), Seiten 156-163, XP011239048, ISSN: 0163-6804, DOI: 10.1109/MCOM.2008.4689259 das ganze Dokument -----	1-13
X	US 2010/031290 A1 (HUA SUZANN [US] ET AL) 4. Februar 2010 (2010-02-04) Zusammenfassung Absatz [0018] - Absatz [0053] Abbildungen 1-5 -----	1-13
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
25. April 2012	04/05/2012

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dujardin, Corinne

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2006 045352 A1 (NOKIA SIEMENS NETWORKS GMBH [DE]) 10. April 2008 (2008-04-10) in der Anmeldung erwähnt Zusammenfassung Absatz [0019] - Absatz [0029] Absatz [0032] - Absatz [0053] Abbildungen 1-2	1-13
X	US 2009/220216 A1 (MARSH CHRISTOPHER [US] ET AL) 3. September 2009 (2009-09-03) Zusammenfassung Absatz [0036] - Absatz [0529] Abbildungen 1-24	1-13
X	WO 2008/113827 A2 (VODAFONE ESPANA SA [ES]; VODAFONE PLC [GB]; ALMENAR BELENGUER PEDRO [E) 25. September 2008 (2008-09-25) Zusammenfassung Seite 6, Zeile 23 - Seite 18, Zeile 28 Abbildung 1	1-13
A	"Hybrid Broadcast Broadband TV ; ETSI TS 102 796 V1.1.1" In: "Hybrid Broadcast Broadband TV ; ETSI TS 102 796 V1.1.1", 1. Juni 2010 (2010-06-01), ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, XP55001426, Seite 7, Zeile 1 - letzte Zeile Seite 11, Zeile 13 - Seite 56, letzte Zeile	7

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2011/060044

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2010031290 A1	04-02-2010	KEINE	
DE 102006045352 A1	10-04-2008	CN 101518029 A	26-08-2009
		DE 102006045352 A1	10-04-2008
		EP 2084883 A1	05-08-2009
		KR 20090067192 A	24-06-2009
		US 2010023962 A1	28-01-2010
		WO 2008037581 A1	03-04-2008
US 2009220216 A1	03-09-2009	KEINE	
WO 2008113827 A2	25-09-2008	ES 2324753 A1	13-08-2009
		WO 2008113827 A2	25-09-2008