(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 102 487 A1** 2014.09.18

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2013 102 487.4**
(22) Anmeldetag: **12.03.2013**
(43) Offenlegungstag: **18.09.2014**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
H04W 12/06 (2009.01)

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(74) Vertreter:
2K Patentanwälte Blasberg Kewitz & Reichel, Partnerschaft, 60325 Frankfurt, DE

(72) Erfinder:
Apeldorn, Andreas Eugen, 65428 Rüsselsheim, DE; Mauerwerk, Mark, 61462 Königstein, DE

(56) Ermittelter Stand der Technik:

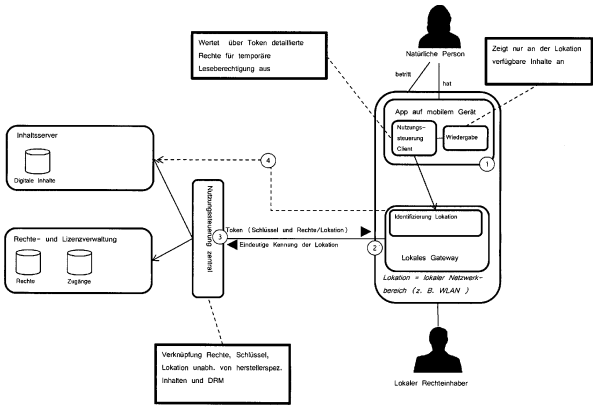
US 2006 / 0 059 096 A1
US 2006 / 0 173 782 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtung zur Steuerung des Zugriffs auf digitale Inhalte**

(57) Zusammenfassung: Verfahren zur Steuerung des Zugriffs auf digitale Daten, umfassend ein mobiles Endgerät mit einer Netzwerkschnittstelle, ein räumlich begrenztes Netzwerksegment, das eine netzwerktechnische Lösung bereitstellt, die zusichert, dass die Lokalisierung des mobilen Endgeräts stattfindet und die Identifikation des Netzwerksegmentes erfolgt kann, ein Nutzungsserver, der den Zugriff auf die digitalen Daten steuert und die Einhaltung spezifischer Rechte zusichert, das Verfahren umfasst die Schritte:
– Erlangen der eindeutigen Identifikation des Netzwerksegmentes, in dem sich das mobile Endgerät befindet,;
– Auswertung der eindeutigen Identifikation an einem Nutzungsserver, der auf der Basis der eindeutigen Identifikation, den Zugriff auf digitale Daten steuert, indem der Anwendung eine Zugriffsliste übergeben wird;
– Anzeigen der digitalen Daten auf dem mobilen Endgerät über die Anwendung.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Steuerung des Zugriffs auf digitale Daten, umfassend ein mobiles Endgerät mit einer Netzwerkschnittstelle und einem räumlich begrenzten Netzwerksegment.

Gebiet der Erfindung:

[0002] Das Prinzip des klassischen, stationären Zugriffs auf digitalisierbare Inhalte (im Allgemeinen eBooks, eMagazine, ePapers, Musik, Videos, Filme, digitale Vouchers e.a. – im Folgenden E-Contents) ist von einer Vielzahl von Anbietern bekannt wie Apple, Amazon etc.. Dieser Ansatz ist jedoch wenig flexibel.

[0003] Aus diesem Grunde wurden bereits Entwicklungen in Richtung von ortsgebundenen Ansätzen verfolgt, die es erlauben an bestimmten Orten bestimmte Inhalte zu lesen bzw. Zugriff auf bestimmte Inhalte bzw. Dienste zu erlangen.

[0004] Die US 20090049057 “METHOD AND DEVICE FOR PROVIDING LOCATION BASED CONTENT DELIVERY” offenbart ein System zum lokationsbasierten Zugriff zur Identifikation von Usern und zur individuellen Bereitstellung von Informationen über Contents.

[0005] Die EP 1274264, EP 127464: „Location Based Content Delivery“ offenbaren eine Lokalisierung, die durch das Endgerät gesteuert wird, in dem eine in dem Endgerät gespeicherte Tabelle aufgerufen wird.

[0006] Bisherige DRM (Digital Rights managment) sind an einzelne User oder Geräte geknüpft. Sog. Location-Aware Access Control Systeme binden DRM und Zugriffskontrolle zwar an bestimmte Lokationen/ Orte – der Rechteinhaber ist dabei selber mobil. Die direkte Bindung von geschützten Inhalten an öffentlich zugängliche Lokationen unabhängig vom momentanen Nutzer ist bisher weder beschrieben noch realisiert – die Lokation ist fix, die Leser können wechseln und dürfen jeweils nur temporär (während der Besuchszeit) die Inhalte, die der lokale Rechteinhaber bereit stellt, verwenden (Metapher = “virtueller Leseraum“). Hieraus ergibt sich, dass es Aufgabe der vorliegenden Erfindung ist, eine solche Steuerung bereitzustellen, die es ermöglicht bestimmte Inhalte einer bestimmten Umgebung zu lesen bzw. darauf zugreifen zu können.

Übersicht über die Erfindung

[0007] Die Erfindung beschreibt eine Lösung für lokationsbasiertes DRM, die einen temporären, ortsabhängigen Zugriff auf geschützte elektronische Multimediainhalte mit Hilfe von mobilen Geräten(im Allgemeinen Smartphones, Tablets, Laptops) unabhängig von einem speziellen Content-Lieferanten erlaubt.

[0008] Gelöst wird diese Aufgabe durch eine Vorrichtung und Verfahren gemäß den Ansprüchen.

[0009] Die Erfindung umfasst ein System und ein Verfahren zur Steuerung des Zugriffs auf digitale Daten. Bei diesen digitalen Daten kann es sich nicht nur um klassische Musikdaten, Videodaten, Spiele oder Informationsdaten in geschriebener Form handeln, sondern es können auch aktive an dem Ort erstellte Inhalte (z.B. Blogs oder Diskussionsforen) gemeint sein, die einen Zugriff für lediglich eine beschränkte Menge von Personen erlauben. Die Erfindung bezieht sich zudem nicht nur auf den Abruf, sondern auch auf die Erstellung von digitalen Inhalten – z.B. Reportagen. Der Begriff Daten ist somit nicht lediglich auf herunterladbaren Inhalt zu begrenzen, sondern kann auch dialogorientierte Foren betreffen, die nicht durch reine Daten in statischer Form gekennzeichnet sind. Weiterhin umfasst die Erfindung ein mobiles Endgerät mit einer Netzwerkschnittstelle, das auf ein räumlich begrenztes Netzwerksegment, das eindeutig einem Rechteinhaber an den in dem Netzwerksegment bereit gestellten digitalen Daten zuordenbar ist. In der Regel handelt es sich hierbei um WLAN Netzwerke, jedoch können auch andere Netzwerke wie Bluetooth, GSM Netzwerke bzw. LTTE oder UMTS Netzwerke gemeint sein, die eine Zellstruktur aufweisen, und somit örtlich begrenzt sind. Diese Netzwerksegmente weisen eine eindeutige Identifikation auf, die in der Regel durch ein Gateway dieses Netzwerksegmentes bereitgestellt wird. Die eindeutige Identifikation des Netzwerksegmentes wird genutzt um die Steuerung des Zugriffes auf die digitalen Daten vorzunehmen.

[0010] Das Verfahren umfasst die Schritte:

– Erlangen der eindeutigen Identifikation des Netzwerksegmentes vom lokalen Gateway, in dem sich das mobile Endgerät befindet, durch eine Anwendung, die die digitalen Daten darstellt;
– Weiterleiten der eindeutigen Identifikation an einen Nutzungsserver, der auf der Basis der eindeutigen Identifikation, den Zugriff auf digitale Daten steuert, indem der Anwendung eine Zugriffsberechtigung übergeben wird;
– Anzeigen der digitalen Daten auf dem mobilen Endgerät über die Anwendung gemäß den vertraglichen Bedingungen der lokal temporär verwendbaren Inhalte.
– Sicheres Löschen der Inhalte, nach dem der Ort bzw. die Reichweite des Netzwerksegmentes verlassen wird, mindestens jedoch nach Erlöschen der temporären Leserechte

[0011] In einer bevorzugten Ausführungsform wird die eindeutige Identifikation des Netzwerksegmentes durch eine Signatur gegenüber dem Nutzungsserver gesichert, so dass ein Missbrauch der Identifikation vermieden wird. So ist die Identifikation des Netz-

werksegmentes mit einer Signatur versehen, die der Nutzungsserver überprüft.

[0012] In einer bevorzugten Ausführungsform stellt der Nutzungsserver einen Token aus, der der Anwendung übergeben wird, nachdem die eindeutige Identifikation erhalten wurde, wobei der Token festlegt, auf welche Daten die Anwendung Zugriff hat, wobei die Anwendung bei jedem Zugriff auf die Daten den Token übermittelt, so dass ein Daten-Server, der die Daten bereitstellt, anhand des Token überprüfen kann, ob die Daten bereitzustellen sind oder nicht. Der Aufbau des Token wird weiter unten beschrieben. Der Token ist in der Regel eine SAML Assertion oder eine vergleichbare Technik die sichere Authentifizierung und Autorisierung ermöglicht. Durch den Token wird festgelegt, welches Netzwerksegment auf welchen Daten Zugriff bekommt. Der Token wird somit für das Netzwerksegment spezifisch zusammengestellt und bildet die Identifikation des Netzwerksegmentes sowie die Rechte des Rechteinhabers in dem Ortsbereiches des Netzwerksegmentes auf die Daten ab, auf die ein Zugriff aus dem Netzwerksegment erfolgen darf.

[0013] Grundsätzlich sind zwei unterschiedliche Szenarien zu betrachten. In einer bevorzugten Ausführungsform läuft die Anwendung als eine Applikation (APP) auf einem mobilen Endgerät ab. Eine solche Anwendung kann z.B. durch bekannte zentrale Stores wie Market Store, AppStore oder Playstore abgerufen werden. Es ist auch denkbar, dass die Anwendung bereits als integraler Bestandteil der Firmware eines mobilen Endgerätes ausgebildet ist. In diesem Falle erfolgt der Zugriff durch die Anwendung auf das Gateway des Netzwerksegmentes, und die Anwendung fordert den Token vom Nutzungsserver an. Die Anwendung weißt in der Regel einen gesicherten Speicherbereich auf (SandBox) in dem die heruntergeladenen Daten abgespeichert werden, soweit dies notwendig ist. Bevorzugt werden natürlich Daten, die nicht lokal abgespeichert werden müssen oder die lediglich durch Streaming erlangt werden müssen, wobei das Wiedergegebene dann vom Gerät verworfen wird. Sollten jedoch die Daten auch lokal gespeichert werden müssen, so erfolgt dies in einem gesicherten Bereich, auf den lediglich die Anwendung Zugriff hat. Dieser Speicherbereich wird durch die Anwendung nach dem Verlassen des Netzwerksegmentes nicht mehr zugänglich gemacht oder gelöscht. Die Anwendung überwacht somit ebenfalls das Eintreten und Austreten in das Netzwerksegment. Ferner verwaltet die Anwendung auch die Beantragung des Token und die Übermittlung des Token an die Server, die die Daten bereitstellen. Die Anwendung stellt somit eine Schnittstelle zu den Komponenten der Erfindung dar. Hierdurch beschafft sich die Anwendung vom Gateway die Identifikation des Netzwerksegmentes, in dem dieses kontaktiert wird.

[0014] In einer alternativen Ausführungsform kann die Anwendung auch auf einem Server laufen und das mobile Endgerät ist lediglich ein Anzeigegerät. Dabei läuft die Anwendung auf einem Server, auf dem das mobile Endgerät mit einem Browser zugreift, wobei die Darstellung lediglich auf dem mobilen Endgerät erfolgt, der Zugriff auf die Daten jedoch durch den Server erfolgt. Es werden somit lediglich Darstellungsdaten übertragen und keine inhaltlichen Daten. Die inhaltlichen Daten bleiben auf dem Anwendungsserver, der die gleiche Funktion aufweist, wie es oben bereits beschrieben wurde.

[0015] Ein (lokales Netzwerksegment), auch ein virtueller Raum genannt, steuert den Zugriff über ein mobiles Gerät auf bestimmte geschützte elektronische Inhalte (E-books, Musik, Dokumente) örtlich und zeitlich begrenzt und vereinigt folgende Eigenschaften:

a) Ein mobiles Gerät mit standardisierter Netzwerktechnologie (z.B. WIFI) wird verwendet um den virtuellen Leseraum zu betreten

b) An das Netzwerk ist ein location basiertes DRM für elektronische Inhalte angebunden

c) Das location basierte DRM ist unabhängig von den verschiedenen Lieferanten für elektronische Inhalte

d) Auf dem mobilen Gerät ist eine Anwendung installiert, die mit dem Netzwerk kommuniziert und das DRM auf dem Lesegerät zusichert.

[0016] Dabei werden folgende Schritte ausgeführt:

1. Das Netzwerk weist einem mobilen Endgerät eine temporäre, lokale Netzwerkadresse zu, dies erfolgt vorzugsweise durch bekannte Mechanismen wie im Falle WIFI durch DHCP. Durch das DHCP kann ebenfalls die Adresse des Gateways mitgeteilt werden, der die entsprechende ID Verwaltung übernimmt. Ferner können Informationen über den Zugriffsserver vermittelt werden, der den Token entsprechend bereitstellt.
2. Die App/Anwendung bekommt eine Zugriffserlaubnis auf die Inhalte mittels eines lokationsspezifischen Token, der nur für den definierten Bereich gültig ist.
3. Über die Anwendung auf dem mobilen Gerät kann an dem Ort des Netzwerksegments auf den Content entsprechend der vertraglichen Regelungen (Bindung an das DRM des spezifischen Content) zugriffen werden.
4. Beim Verlassen des virtuellen Leseraumes wird der lokationsspezifische Token einschließlich etwaiger zwischengespeicherter Inhalte von der App gelöscht und damit der weitere Zugriff auf die Inhalte verhindert
5. Über Sicherheitsmechanismen am lokalen Netzwerk wird die missbräuchliche Nutzung des Content verhindert
6. Ein Mechanismus der den Token ungültig macht, wenn bestimmte lokale Informationen feh-

len (z.B. MAC-Adresse, des Gateways) oder IP-Adresse,

7. die App Mechanismen enthält, die auf Wunsch den Erwerb persönlicher Rechte am Content für die Mitnahme erlaubt. In einer weiteren Ausbildungform ist es auch möglich, dass der Anwender den Inhalt mitnehmen kann, indem er diesen entsprechend erwirbt oder andere Erklärungen bzw. Einwilligungen abgibt.

[0017] Mit der Erfindung können in Lokationen/Ortsbereichen mit kabellosem Netzempfang (i.e. Wi-Fi) geschützte E-Contents temporär freigeschaltet werden. Der Besitzer eines mobilen Gerätes (insb. Smartphones, Tablets & Notebooks) kann in vollem Umfang ohne Authentifizierung auf den E-Content zugreifen, sobald – und solange – er sich in der Lokation aufhält. Verlässt er die Lokation, verfällt auch der Zugriff – es sei denn, der User hat den Content erworben. Das Digital Rights Mangement ist an die Lokation gebunden.

[0018] Die Idee eines providerunabhängigen, lokationsabhängigen Zugriffs auf Content verknüpft für jeden Nutzer eines mobilen Gerätes die Vorteile des Online Handels (Zugriff auf Contens mit dem eigenen Device) mit den Vorteilen des stationären Handels (i.e. persönliche Beratung, Unterstützung der Kaufentscheidung durch Betrachten und Bewerten des Inhalts). Außerdem bietet lokationsbasierter Zugriff auf Content neue

– Servicekonzepte (i. E. "elektronischer Lesezirkel", Zugriff auf e-Contents in Büchereien, Zugriff auf Videos, Musik, Hörbücher etc. mit dem eigenen Gerät in Zügen, Flugzeugen etc.)

– und neue Vertriebskonzepte (i. E. eKiosks auf Bahnsteigen, in Hotels, in Unternehmensniederlassungen, Flughäfen...)

– Marketingkonzepte (i.e. Gutscheine, die nur innerhalb einer Lokation verfügbar sind)

Figurenbeschreibung:

[0019] Die Figuren zeigen mögliche Ablaufdiagramme der vorliegenden Erfindung.

[0020] Fig. 1 zeigt ein Verfahren mit einer Anwendung auf einem mobilen Endgerät, die einen Token erhält;

[0021] Fig. 2 zeigt ein Verfahren, bei dem der Informationsfluss hinsichtlich der verwendeten Funktionen beschrieben wird;

[0022] Fig. 3 zeigt die Ablaufschritte auf der Anwendung und deren Benutzerinteraktion;

[0023] Fig. 4 zeigt ein Ablaufdiagramm der Anwendung.

Beschreibung der Ausführungsform

[0024] Die **Fig.** 1 zeigt den möglichen Ablauf des Verfahrens. Die folgenden Schritte sind zu beachten.

1. Ein potentieller Kunde als natürliche Person betritt mit seinem Gerät, auf dem die Anwendung als WebApp ausgeführt wird, den „virtuellen Lese-Raum“/Netzwerksegment und bekommt dynamisch eine lokale Netzwerkadresse zugewiesen.
2. Die App sendet, sobald die lokale Netzwerkadresse zugewiesen ist, eine Nutzungsanfrage an die zentrale Nutzungssteuerung. Die Adresse für die zentrale Nutzungsteuerung kann ebenfalls aus den DHCP Informationen erlangt werden. Da die Nutzungsrechte der geschützten Inhalte über den lokalen Rechteinhaber gehalten werden, ist eine lokale Zugriffssteuerung erforderlich. Um Missbrauch zu vermeiden, kommen ggf. weitere Schutzmechanismen zur Absicherung der Kommunikation mit der zentralen Nutzungssteuerung über das lokale Gateway zum Einsatz (z.B. Authentifizierungstechniken wie HMAC, RFC 2104). Die zentrale Nutzungssteuerung ermittelt Rechte und Zugänge für den Zugriff der Lokation auf den Inhaltsserver und generiert einen lokationsspez. Token, der an die APP übergeben wird.
3. Nur mit dem Token erhält das mobile Gerät temporäre Leseberechtigung. Die App stellt sicher, dass nach Ablauf der Leseberechtigung (i.R. nach Verlassen des lokalen Netzes) der Token verfällt und der Zugriff auf den Content wird durch die lokale Nutzungssteuerung verhindert.

[0025] Eine Übersicht über den Inhalt stellt ebenfalls die App bereit, hierbei werden zum Beispiel in Kategorien und Listen unterschiedliche Bereiche und Arten von Inhalten angezeigt, die der Benutzer dann über eine Menüstruktur auswählen kann.

[0026] Die in den Schaubildern dargestellte Verteilung der Komponenten stellt jeweils eine der möglichen Varianten dar. Die Einhaltung der digitalen Rechte erfordert das Zusammenspiel zwischen der lesenden Anwendung (entweder auf dem Client oder als Web-Anwendung) und der zentralen Nutzungssteuerung, die den Zusammenhang zwischen dem Rechteinhaber an der Lokation, der eindeutig identifizierten Lokation und den Zugriff auf die entsprechend der vertraglichen Regelungen zugesicherten multimedialen Inhalte regelt. Logisch sind dazu folgende Komponenten erforderlich:

• Lesende App: Entweder auf dem mobilen Endgerät als Thick Client oder als Web-Anwendung. Das Zusammenspiel mit der zentralen Nutzungsteuerung muss entsprechend abgesichert sein, damit die Einhaltung der digitalen Rechte zugesichert werden kann

• Zentralle Nutzungssteuerung: Die Zentrale Nutzungssteuerung mapped die Identifyer der Lokationen auf die jeweiligen Zugänge der Rechteinha-

ber (Authentifizierung), wertet die Rechte an den Inhalten aus (Autorisierung) und liefert dem Client einen entsprechenden Token für den Zugriff auf die Inhalte zurück. Je nach nichtfunktionalen Gegebenheiten kann der Zugriff direkt vom Client oder über das Gateway erfolgen. Zur Absicherung kommen gängige Verschlüsselungsmechanismen wie SSL in synchronen oder asynchronen Verfahren zum Einsatz.

• Zugänge: Die Zugänge werden in der Regel über einen Verzeichnisdienst im Rahmen eines Identity Management verwaltet. Da unterschiedliche Contentarten zum Einsatz kommen, sind auch entsprechend unterschiedliche Zugangsarten zu verwalten.

• Gateway: Die technische Komponente, die die Vergabe einer lokationsspezfischen ID sicherstellt. Die ID kann dabei beliebig zusammengesetzt sein (z.B. ein für die Lokation eindeutiger Netzwerkbereich oder ein Identifier, der vom Netzwerkprovider eindeutig zugeteilt wird, wie Location ID oder Service ID). Diese, das lokale Netzwerk identifizierende ID, wird dem Client auf Anfrage in der Response/Antwort mitgeteilt und wird von der zentralen Nutzungssteuerung auf den tatsächlichen Rechteinhaber an der Lokation gemapped.

• Inhaltsserver/Digitale Inhalte: Die Inhalte werden vom Content-Lieferanten zur Verfügung gestellt. Die zentrale Nutzungsteuerung stellt gemäß den vertraglichen und technischen Gegebenheiten im Zusammmenspiel mit den Content-Lieferanten den ordnungsgemäßen Zugriff sicher. Der Zugriff erfolgt entweder auf entsprechend vorprozessierte Inhalte direkt auf ein Repository oder über eine Schnittstellentechnik auf die Inhalte.

• Lokation: Grundsätzliche alle lokal begrenzte Netzwerkbereiche, die eindeutig lokalisierbar sind. Folgende Netzwerktechnologien bieten sich nach heutigem Stand der Technik an:

– DSL
– Jeder lokalisierbare WIFI-Netzwerkbereich
– HotSpot
– Mobile Zellen, insbes. eindeutig räumlich begrenzbare Pico- oder Femtozellen
– Geocaching
– Bluetooth
– NFC

[0027] Die Nutzungssteuerung an der Lokation kann entweder als Web-Lösung mit der Kernfunktionalität im Gateway oder als App (Thick Client) mit der Kernfunktionalität in der App realisiert werden. In jedem Fall liegt die Verteilung der Komponenten der lokationsspez. Nutzungssteuerung (z.B. über App Store oder Gateway als Appliance) im Verantwortungsbereich des Plattformanbieters und bildet ein in sich geschlossenes System. Eine der möglichen Verteilungen ist im Schaubild dargestellt.

[0028] Das Token enthält inhaltlich im Wesentlichen die Information einer SAML Assertion (Security Assertion Markup Language), ein Standard zum Austausch von Authentifizierungs- und Autorisierungsinformationen, Bsp. siehe Anhang, Referenz zum Standard: https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=security).

[0029] Da im Sinne eines DRM alle Komponenten zur Nutzungskontrolle durch uns als Service Provider angeboten werden sollen, kann intern mit einer symmetrischen Signatur unter Verwendung eines shared Secret gearbeitet werden. Wenn allerdings die Komponenten bei unterschiedlichen Anbietern stehen, so kann auch ein anderes Verfahren verwendet werden.

[0030] Eine Bindung an das Gateway ist hier logisch gemeint. Technisch kann das Gateway je nach Einsatzszenario auch außerhalb der Kontrolle der Nutzungssteuerung sein.

[0031] Die eigentliche Steuerung des Zugriffs auf die Inhalte erlaubt nur die zentrale Nutzungssteuerung. Das Gateway ist grundsätzlich nichts anderes als ein lokales „Einganstor“ für das mobile Gerät. Allerdings muss netzwerktechnisch die „Location“ identifiziert werden. Das Gateway liefert an die App die sog. „Location ID“. Die Ermittlung der ID muss abgesichert sein. Nur wenn die App eine gesicherte Location-ID hat, bekommt sie von der zentralen Nutzungssteuerung den Token. Das Gateway bezeichnet hier somit logisch eine netzwerktechnisch Lösung, die zusichert, dass die Lokalisierung des mobilen Endgeräts stattfindet und die Lokation eindeutig identifiziert werden kann.

[0032] Nur die zentrale Nutzungssteuerung hat Kenntnis über die den Lokationen zugeordneten Rechteinhaber und ermittelt dementsprechend die Inhalte.

[0033] Das ist hier generisch formuliert, da wir außer WLAN auch weitere Netzwerktechnologien nutzen wollen (z.b. Picozellen, Geocaching, Bluetooth, NFC – s.o.). D.h. die Logik des Mechanismus bleibt überall gleich, nur die konkrete technische Umsetzung kann variieren.

[0034] Die App zeigt nur die an der Lokation verfügbaren Inhalte (Metapher “lokales Bücherregal“) vorbehaltlich, dass sie einen gültigen Token bekommt und stellt sicher, dass nach dem Verlassen der Lokation (Erlöschen der Leseberechtigung), kein weiterer Zugriff möglich ist.**Fig.** 2 zeigt den sequentiellen Ablauf unter Verwendung der oben beschriebenen logischen Komponenten:

• Nachdem der Anwender mit seinem mobilen Gerät, den lokalen Netzwerkbereich betreten hat, fordert die App einen eindeutigen Identifier für die Lokation am Gateway an.

- Im nächsten Schritt sendet die App über eine verschlüsselte Verbindung die Netzwerk ID an die zentrale Nutzungssteuerung.
- Die Zentrale Nutzungssteuerung ermittelt die ID des Rechteinhabers an der Lokation und erfragt beim IDM die Zugriffsrechte auf geschützte elektronische Inhalte. Das temporäre Token wird an die App zurückgesendet.
- Mit dem temporären Token erhält die App Zugriff auf die an der Lokation verfügbaren Inhalte. Ob die App direkt Zugriff auf den/die Content-Server erhält hängt von den netzwerktechnischen Gegebenheiten ab. In der Praxis sind je nach Schutzbedarfsanforderung verschiedene Schutzmechanismen denkbar.

[0035] Die Abbildungen **Fig.** 3–**Fig.** 5 zeigen wie die Technologie innerhalb einer App verwendet werden kann, die ortsgebunden elektronische Bücher, Zeitungen oder Hörbücher bereitstellt. Die **Fig.** 3 zeigt Folgendes: Nach dem Öffnen der Anwendung bekommt der Benutzer entweder

a) Sofort und ohne weitere, persönliche Autorisierung die für diese Lokation freigeschalteten Inhalte angezeigt, sofern das verwendete Netzwerk durch das in **Fig.** 2 beschriebene Verfahren und hier als „Beziehe Token“ beschriebene Verfahren autorisiert wird, um auf Inhalte zuzugreifen („Zeige Inhaltsübersicht“).

b) Einen Lokation Finder angezeigt, der darstellt welche Inhalte an welchen Lokationen verfügbar sind.

c) Eine Einleitung zum erstmaligen Gebrauch der Anwendung angezeigt, sofern er die Anwendung zum ersten Mal öffnet.

[0036] Die **Fig.** 4 zeigt, dass der Benutzerim Falle einer Autorisierung die Inhalte vollständig einsehen und nutzen kann.

[0037] Im Hintergrund (**Fig.** 5) überprüft die App regelmäßig, ob die Autorisierung noch Bestand hat, indem sie die Gültigkeit des Tokens prüft. Ist der Token noch gültig, können die Inhalte weiter verwendet werden. Ist der Token nicht mehr gültig, erscheint eine Warnmeldung. Gleichzeitig wird die Zeit ohne gültigen Token bis zu einem festgelegten Grenzwert aufaddiert. Liegt die Zeit ohne gültigen Token über dem Grenzwert („Zeitverzögerung ohne gültigen Token über dem Grenzwert?“), werden die Inhalte aus dem Cache gelöscht („Entferne Inhalte“). Es erscheint wieder der Lokationsfinder.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- US 20090049057 [0004]
- EP 1274264 [0005]
- EP 127464 [0005]

Zitierte Nicht-Patentliteratur

- RFC 2104 [0024]
- https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=security) [0028]

Patentansprüche

1. Verfahren zur Steuerung des Zugriffs auf digitale Daten, umfassend ein mobiles Endgerät mit einer Netzwerkschnittstelle, ein räumlich begrenztes Netzwerksegment, dass eine netzwerktechnische Lösung bereitstellt, die zusichert, dass die Lokalisierung des mobilen Endgeräts in dem Netzwerksegment stattfindet und die Identifikation des Netzwerksegmentes erfolgen kann, ein Nutzungsserver, der den Zugriff auf die digitalen Daten steuert und die Einhaltung spezifischer Rechte zusichert, das Verfahren umfasst die Schritte:
– Erlangen der eindeutigen Identifikation des Netzwerksegmentes, in dem sich das mobile Endgerät befindet,;
– Auswertung der eindeutigen Identifikation an einem Nutzungsserver, der auf der Basis der eindeutigen Identifikation den Zugriff auf digitale Daten steuert, indem der Anwendung eine Zugriffsliste übergeben wird;
– Anzeigen der digitalen Daten auf dem mobilen Endgerät über die Anwendung.

2. Das Verfahren nach dem vorhergehenden Anspruch, wobei die eindeutige Identifikation des Netzwerksegmentes durch eine Signatur gegenüber dem Nutzungsserver gesichert wird, so dass ein Missbrauch der Identifikation vermieden wird.

3. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei der Nutzungsserver einen Token ausstellt, der der Anwendung übergeben wird, nachdem die eindeutige Identifikation erhalten wurde, wobei der Token festlegt, auf welche Daten und unter welchen Bedingungen die Anwendung Zugriff hat, wobei die Anwendung bei jedem erneuten -Zugriff auf die Daten den Token übermittelt, so dass ein Daten-Server, der die Daten bereitstellt, anhand des Token überprüfen kann, ob die Daten bereitzustellen sind oder nicht.

4. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei die Anwendung auf einem Server läuft, auf den das mobile Endgerät mit einem Browser zugreift, wobei die Darstellung lediglich auf dem mobilen Endgerät erfolgt, der Zugriff auf die Daten jedoch durch den Server erfolgt.

5. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei die Anwendung auf dem mobilen Endgerät läuft und den Zugriff auf die Daten über die Anwendung erfolgt.

6. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei die Daten, nachdem sie durch die Anwendung heruntergeladen wurden, in einem durch die Anwendung gesicherten Bereich und/oder Sandbox zwischengespeichert werden, wobei ein Zugriff auf diesen gesicherten Bereich nur mit einem zulässigen Token möglich ist.

7. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei der Token seine Gültigkeit verliert, wenn das mobile Endgerät das Netzwerksegment verlässt.

8. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei die Anwendung vom lokalen Netzwerksegment mit Hilfe eines Gateways, der den Zugriff auf das Netzwerksegment und die Identifikation des Netzwerks verwaltet, die Identifikation des Netzwerksegmentes erlangt, indem dieser kontaktiert wird.

9. Das Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, wobei die elektronischen Inhalte auch direkt im lokalen Netzwerk der Lokation abgelegt sein können, sofern die Lokation selber die Einhaltung der digitalen Zugriffsrechte sicherstellen kann und gleichzeitig eigenständig die abgesicherte Kommunikation mit dem Client durchführen kann.

10. System umfassend ein mobiles Endgerät und einen Zugriffs-Server und ein räumlich begrenztes Netzwerksegment, gekennzeichnet durch eine Struktur und Einrichtung, die den Ablauf des Verfahrens nach einem oder mehreren der vorhergehenden Verfahrens-Ansprüche.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

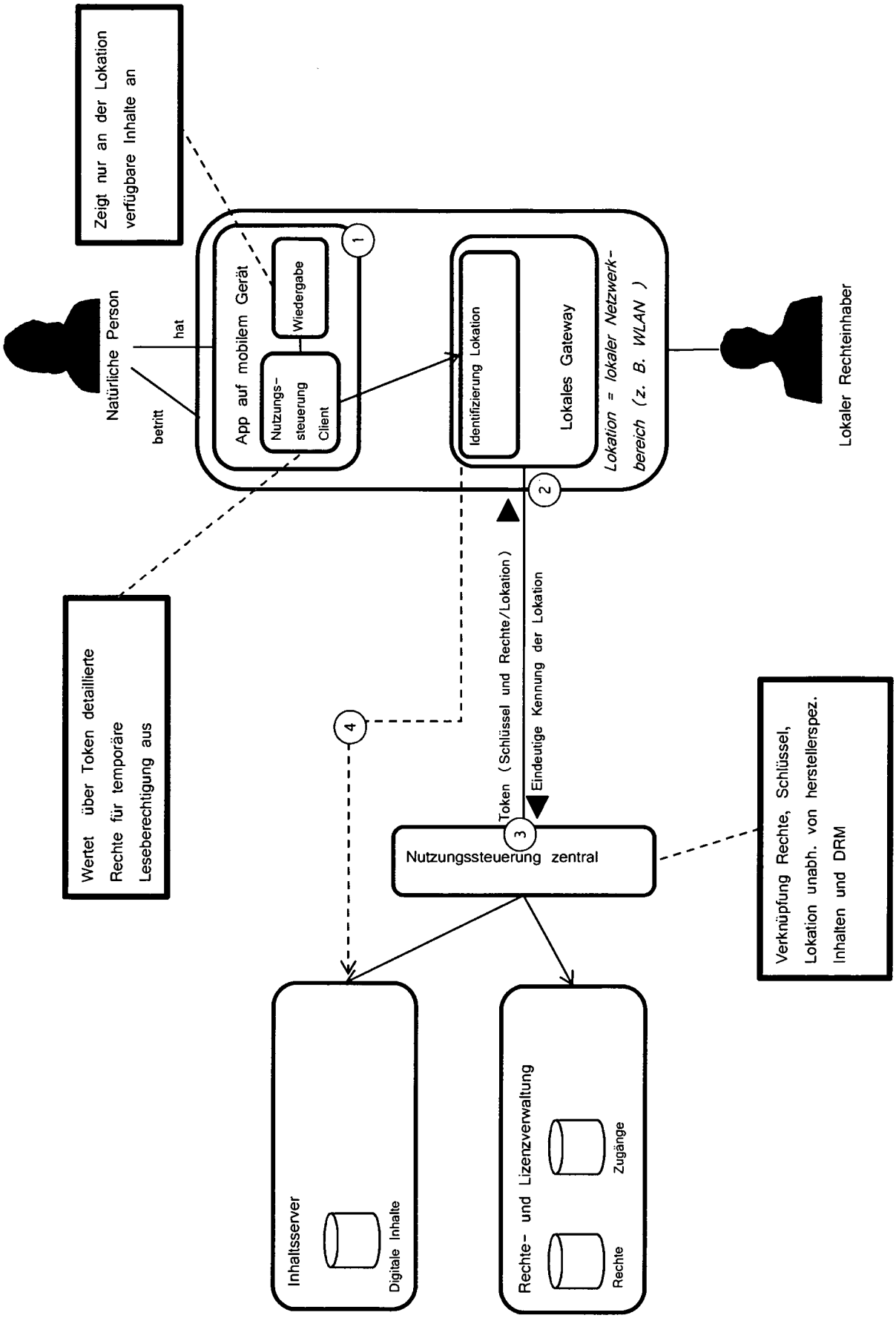


Fig. 1

Fig. 2

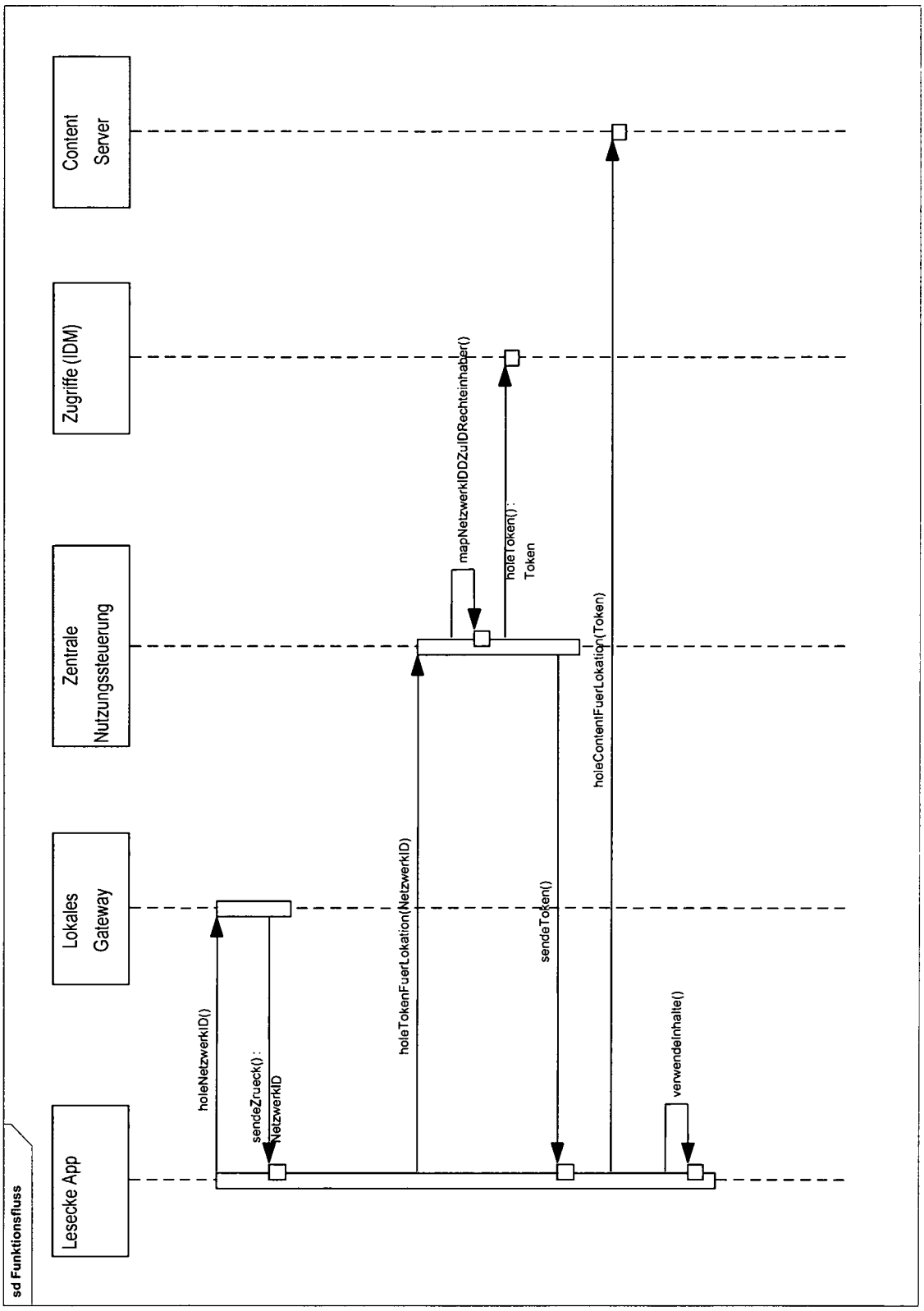

sd Funktionsfluss
Lesecke App
Lokales Gateway
Zentrale Nutzungssteuerung
Zugriffe (IDM)
Content Server
holeNetzwerkID()
sendeZrueck() : NetzwerkID
holeTokenFuerLokation(NetzwerkID)
mapNetzwerkIDDZuIDRechteinhaber()
holeToken() : Token
sendeToken()
holeContentFuerLokation(Token)
verwendeInhalte()

Fig. 3

Beispiel App Anwendung

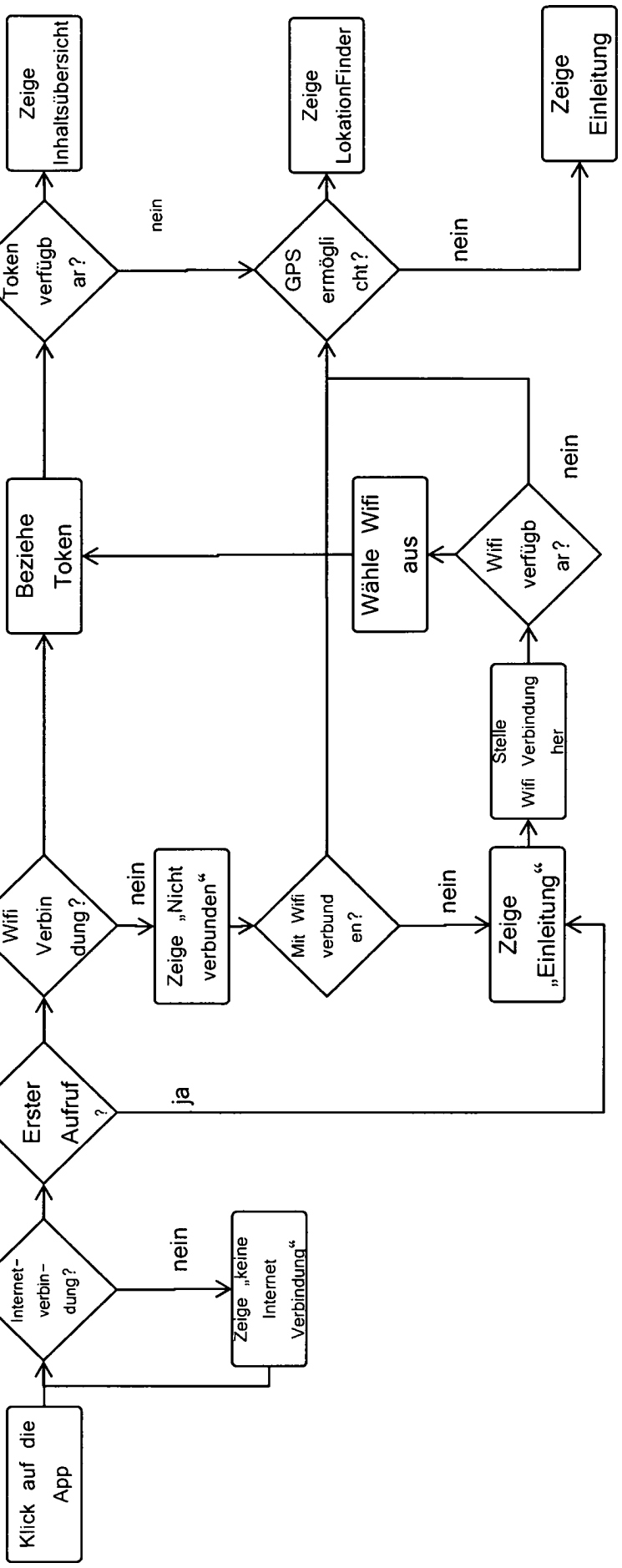


Fig. 4

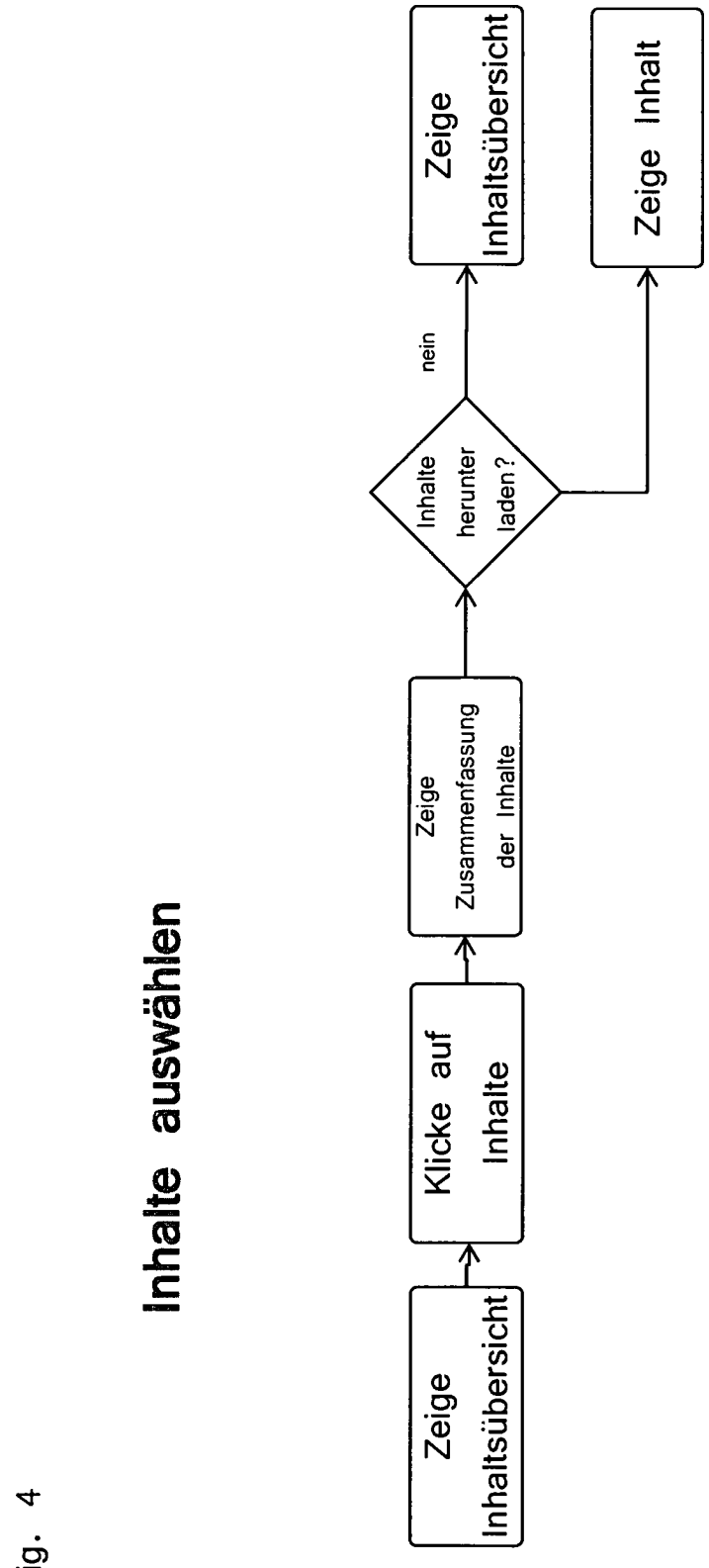
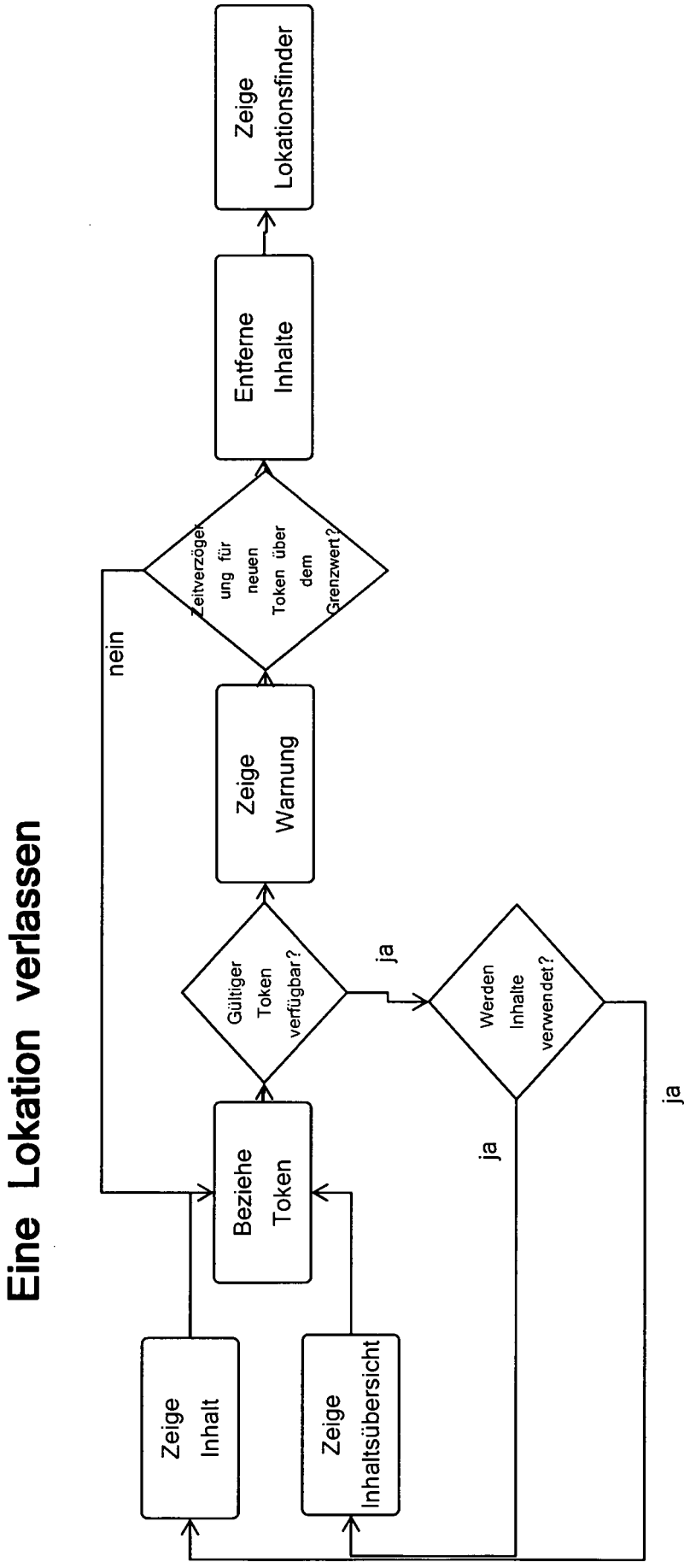

Inhalte auswählen
Zeige Inhaltsübersicht
Klicke auf Inhalte
Zeige Zusammenfassung der Inhalte
Inhalte herunter laden?
nein
Zeige Inhaltsübersicht
Zeige Inhalt

Fig. 5


Eine Lokation verlassen
Zeige Lokationsfinder
Entferne Inhalte
Zeitverzögerung für neuen Token über dem Grenzwert?
nein
Zeige Warnung
Gültiger Token verfügbar?
ja
Werden Inhalte verwendet?
ja
ja
Beziehe Token
Zeige Inhalt
Zeige Inhaltsübersicht