

(12) **Österreichische Patentanmeldung**

(21) Anmeldenummer: A 1053/2012
(22) Anmeldetag: 27.09.2012
(43) Veröffentlicht am: 15.04.2014

(51) Int. Cl.: **H04W 12/06** (2009.01)
H04W 52/02 (2009.01)
H04L 9/32 (2006.01)
H04B 5/02 (2006.01)

(56) Entgegenhaltungen:
US 2008182592 A1
US 2011087887 A1

(71) Patentanmelder:
Phactum Softwareentwicklung GmbH
1080 Wien (AT)

(72) Erfinder:
Minichmayr Markus
1180 Wien (AT)

(74) Vertreter:
WILDHACK & JELLINEK PATENTANWÄLTE
OG
WIEN

(54) **Verfahren und Vorrichtung zum Zugriff auf eine Netzwerkressource durch ein mobiles Endgerät mit zeitlicher und lokaler Begrenzung**

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung welche einem Benutzer mit Hilfe eines mobilen Endgerätes, über ein Netzwerk, insbesondere das Internet, den Zugriff auf eine Ressource ermöglichen, wobei dieser Zugriff durch einen Server gesteuert wird, welcher zuverlässig feststellen kann, ob das mobile Endgerät sich zum ungefähren Zeitpunkt der Überprüfung in der Nähe eines Schlüsselmechanismus befindet. Die Identität der Ressource und des Servers werden durch den vorgenannten Schlüsselmechanismus festgelegt, das mobile Endgerät muss nicht manuell auf die konkrete Ressource eingestellt werden. Der Schlüsselmechanismus stellt dazu Zugriffsdatensätze aus (z.B. in Form von URLs), welche die Ressource identifizieren, einen zeitlichen Bezug aufweisen und digital signiert sind. Diese werden über eine lokale Datenverbindung (z.B. NFC) an das mobile Endgerät versandt welches diese vorzugsweise automatisiert verarbeitet und damit auf die Ressource zugreifen kann, wobei der Server die Signatur und die zeitliche Nähe prüft und anhand dieser den Zugriff steuert.

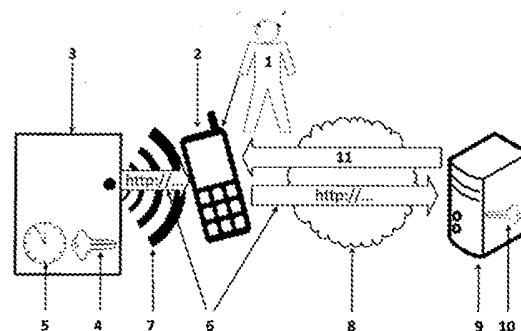


Fig. 1

Zusammenfassung:

Die Erfindung betrifft ein Verfahren und eine Vorrichtung welche einem Benutzer mit Hilfe eines mobilen Endgerätes, über ein Netzwerk, insbesondere das Internet, den Zugriff auf eine Ressource ermöglichen, wobei dieser Zugriff durch einen Server gesteuert wird, welcher zuverlässig feststellen kann, ob das mobile Endgerät sich zum ungefähren Zeitpunkt der Überprüfung in der Nähe eines Schlüsselmechanismus befindet. Die Identität der Ressource und des Servers werden durch den vorgenannten Schlüsselmechanismus festgelegt, das mobile Endgerät muss nicht manuell auf die konkrete Ressource eingestellt werden. Der Schlüsselmechanismus stellt dazu Zugriffsdatensätze aus (z.B. in Form von URLs), welche die Ressource identifizieren, einen zeitlichen Bezug aufweisen und digital signiert sind. Diese werden über eine lokale Datenverbindung (z.B. NFC) an das mobile Endgerät versandt welches diese vorzugsweise automatisiert verarbeitet und damit auf die Ressource zugreifen kann, wobei der Server die Signatur und die zeitliche Nähe prüft und anhand dieser den Zugriff steuert.

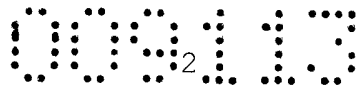
(Fig. 1)

Die Erfindung betrifft ein Verfahren zum Zugriff auf eine Netzwerkressource durch ein mobiles Endgerät mit zeitlicher und lokaler Begrenzung.

Die Erfindung betrifft des Weiteren eine Vorrichtung zum Zugriff auf eine Netzwerkressource durch ein mobiles Endgerät mit zeitlicher und lokaler Begrenzung, wobei die Netzwerkressource (in weiterer Folge einfach „Ressource“) durch einen Schlüsselmechanismus identifiziert wird, und wobei das mobile Endgerät über Mittel verfügt, Daten von Geräten in dessen lokaler Umgebung zu empfangen, sowie über Mittel zur Herstellung einer Verbindung zu einem Netzwerk, insbesondere dem Internet. Das mobile Endgerät verfügt idealer Weise über eine elektronische Benutzerschnittstelle, insbesondere ein grafisches Display, ein Touchscreen oder dergleichen.

Die Erfindung sieht des Weiteren einen Server vor, welcher den Zugriff durch das mobile Endgerät (z.B. Smartphone, Tablet-PC, Rechner, Fahrzeug, etc.) auf die durch den Schlüsselmechanismus identifizierte Ressource steuert, insbesondere den Zugriff ermöglichen oder verhindern kann. Das Verfahren ist so konzipiert, dass es einem Benutzer erlaubt, gegenüber diesem Server glaubhaft zu machen, dass der Benutzer bzw. dessen mobiles Endgerät sich zum Zeitpunkt der Ausführung des Verfahrens in lokaler Nähe zum genannten Schlüsselmechanismus befindet oder kurz davor befunden hat. Es ist vorgesehen, dass der Server den Zugriff auf die identifizierte Ressource nur dann ermöglicht, wenn diese Voraussetzung gegeben ist.

Die Identität der Ressource, auf welche Zugriff gewährt werden soll, sowie des Servers, welcher den Zugriff steuert, wird dem



mobilen Endgerät durch den Schlüsselmechanismus bekanntgegeben und kann somit von diesem Schlüsselmechanismus gesteuert werden. Das mobile Endgerät und der Server verfügen über Mittel, die es dem mobilen Endgerät ermöglichen, über ein Netzwerk eine Verbindung zum Server herzustellen. Die konkrete Identität des Servers selbst muss dem mobilen Endgerät am Anfang der Ausführung des Verfahrens jedoch noch nicht bekannt sein, sondern das mobile Endgerät erfährt die Identität des Servers und der Ressource vom vorgenannten Schlüsselmechanismus. Dadurch wird es einem Benutzer im Rahmen des gegenständlichen Verfahrens mit Hilfe seines mobilen Endgerätes möglich, auf unterschiedliche Server bzw. Ressourcen zuzugreifen, ohne dass das mobile Endgerät zuvor jeweils auf diese eingestellt werden müsste. Die Verknüpfung mit einem bestimmten Server bzw. einer bestimmten Ressource liegt alleine am Schlüsselmechanismus.

Im Sinne dieser Erfindung bringt der Benutzer das mobile Endgerät in die Nähe des Schlüsselmechanismus, sodass das mobile Endgerät Daten vom Schlüsselmechanismus empfangen kann (z.B. per Near Field Communication (NFC), RFID, Bluetooth, dynamisch generierte optische Barcodes, etc.). Der Schlüsselmechanismus erzeugt, entweder angeregt durch die lokale Nähe des mobilen Endgeräts oder aber ständig, ohne die lokale Nähe eines mobilen Endgerätes zu berücksichtigen, ein Datenpaket, in weiterer Folge digitaler Zugriffsdatensatz genannt, das folgende Eigenschaften aufweist:

- Der digitale Zugriffsdatensatz enthält einen Verweis auf den Server, der den Zugriff steuern soll sowie einen Verweis auf die konkrete Ressource, auf die Zugriff gewährt werden soll.
- Der digitale Zugriffsdatensatz ist so gestaltet, dass der Server feststellen kann, ob dieser in zeitlicher Nähe zum Zeitpunkt der Autorisierung erstellt wurde.

009₃13

- Der digitale Zugriffsdatensatz ist so gestaltet, dass der Server feststellen kann, dass der Zugriffsdatensatz von einem Schlüsselmechanismus ausgestellt wurde, dem der Server vertraut.

Der Zugriffsdatensatz ist idealer Weise so gestaltet, dass er vom mobilen Endgerät automatisch verarbeitet werden kann und das mobile Endgerät ist idealer Weise ausgebildet, solche Zugriffsdatensätze automatisch zu verarbeiten. Der Zugriffsdatensatz kann z.B. als einheitlicher Quellenanzeiger (uniform resource locator, URL) ausgeprägt sein, der die zuvor genannten Eigenschaften aufweist und der das mobile Endgerät veranlasst, die entsprechende Webseite in einem Web-Browser zu öffnen und anzuzeigen.

Der Zugriffsdatensatz wird vom mobilen Endgerät zum Server übertragen und von diesem auf Korrektheit geprüft, insbesondere wird überprüft, ob der Zugriffsdatensatz in zeitlicher Nähe zum Zeitpunkt der Überprüfung ausgestellt wurde und ob der Zugriffsdatensatz von einem Schlüsselmechanismus ausgestellt wurde, dem der Server vertraut. Wird der Zugriffsdatensatz vom Server akzeptiert, gibt dieser den Zugriff auf die identifizierte Ressource frei. Der Zugriff durch das mobile Endgerät auf die identifizierte Ressource inklusive möglicher zusätzlicher Autorisierungsschritte erfolgt in weiterer Folge nach bekannten Verfahren.

Bereits bekannt ist die Nutzung von Hardwaremodulen, die zeitlich begrenzt gültige Zugriffsschlüssel erzeugen (z.B. RSA Secure ID). Ebenfalls bereits bekannt ist die Nutzung von Hardwaremodulen zur Erzeugung von Einmalpassworten, die von mobilen Endgeräten über lokale Datenverbindungen (z.B. per NFC) ausgelesen werden können.

Die Aufgabe der vorliegenden Erfindung besteht in der Schaffung eines oben genannten Verfahrens und einer oben genannten Vorrichtung mit deren Hilfe dem Benutzer eines mobilen Endgerätes besonders einfach Zugriff auf eine durch einen Schlüsselmechanismus identifizierte Ressource erteilt werden kann, wobei der beteiligte Server darauf vertrauen kann, dass sich das mobile Endgerät zum Zeitpunkt der Autorisierung oder zumindest kurz davor in lokaler Nähe zum Schlüsselmechanismus befindet oder befunden hat. Durch diese neuartige Kombination wird eine Klasse von Anwendungen möglich, die bei Nutzung herkömmlicher Verfahren und Vorrichtungen nicht möglich wäre.

Ein Anwendungsbeispiel für das gegenständliche Verfahren bzw. die gegenständliche Vorrichtung ist die Nutzung in einem Restaurant zur Bestellung von Speisen und Getränken durch Gäste. Auf jedem Tisch ist in der Tischplatte ein Schlüsselmechanismus gemäß der gegenständlichen Erfindung integriert, wobei dieser optisch so markiert ist, dass dessen Zweck für Gäste erkennbar ist. Bei der vom Schlüsselmechanismus identifizierten Ressource handelt es sich um eine Website, auf der das Restaurant Bestellungen für den konkreten Tisch entgegennimmt. Ein Restaurantbesucher bringt sein Mobiltelefon in die Nähe des Schlüsselmechanismus, sodass es Daten von diesem empfangen kann (z.B. per NFC). Der Schlüsselmechanismus versendet in diesem Beispiel eine URL, die auf den Webserver des Restaurants und darauf auf die Webseite des jeweiligen Tisches verweist. Die URL enthält außerdem weitere Daten entsprechend der gegenständlichen Erfindung, konkret Datum und Uhrzeit zum Zeitpunkt der Ausstellung der URL und eine Signatur, die mit dem privaten Schlüssel des Schlüsselmechanismus erstellt wurde über welchen nur dieser verfügt. Das Mobiltelefon öffnet daraufhin in einem Web-Browser die empfangene URL bzw. die entsprechende Webseite

009:13

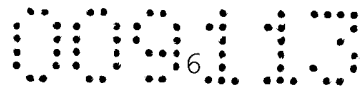
auf der für den konkreten Tisch Speisen und Getränke bestellt werden können. Die Website bzw. der Server prüft die in der URL enthaltenen Daten und leitet auf die Bestellseite des jeweiligen Tisches (Ressource) um, sofern der Zugriffsdatensatz (die URL) entsprechend des gegenständlichen Verfahrens als gültig bewertet wird (lokale und zeitliche Nähe sowie gültige Signatur). Da das Verfahren bei erfolgreicher Durchführung sowohl lokale Nähe des Endgerätes zum Schlüsselmechanismus garantiert, der in diesem Beispiel im Tisch integriert ist, als auch, dass die lokale Nähe zeitlich nahe am Zeitpunkt der Bestellung lag, kann das Restaurant beim Eingang einer Bestellung mit ausreichender Sicherheit davon ausgehen, dass die Bestellung von den Personen kommt, die zum Zeitpunkt der Bestellung am in der Bestellung genannten Tisch sitzen. Durch die Verwendung von Standardtechnologien (in diesem Beispiel NFC, URL, Web Browser, Internet am Smartphone), kann ein Benutzer eine entsprechende Vorrichtung nutzen, ohne sein mobiles Endgerät (z.B. sein Smartphone) konkret auf die Bestellung von Speisen und Getränken oder ein bestimmtes Restaurant vorzubereiten. Stattdessen können mit demselben mobilen Endgerät unterschiedliche derartige Vorrichtungen (z.B. in unterschiedlichen Restaurants) genutzt werden, ohne dass das mobile Endgerät jeweils manuell für den jeweiligen Fall konfiguriert werden müsste.

Die Erfindung wird anhand der beigefügten Zeichnungen näher erläutert. Darin zeigen:

Fig. 1 ein schematisches Blockdiagramm einer erfindungsgemäßen Vorrichtung

Fig. 2 ein schematisches Ablaufdiagramm eines erfindungsgemäßen Verfahrens

Fig. 1 zeigt ein schematisches Blockdiagramm einer erfindungsgemäßen Vorrichtung welche einem Benutzer 1 mit



Hilfe dessen mobilen Endgerätes 2 den Zugriff auf eine Ressource 11 ermöglicht, wobei diese Ressource 11 von einem Schlüsselmechanismus 3 identifiziert wird. Der Schlüsselmechanismus 3 ist in der Lage, Zugriffsdatensätze 6 zu erstellen, welche Zugriffsdatensätze 6 einen Verweis auf den Server 9, die identifizierte Ressource 11 sowie einen Hinweis auf den Ausstellungszeitpunkt enthalten, welchen Ausstellungszeitpunkt der Schlüsselmechanismus 3 von einem Zeitgeber 5 erhält. Vorteilhafter Weise enthält der Zugriffsdatensatz des Weiteren einen Hinweis auf die Identität des Schlüsselmechanismus 3, sodass bei einer späteren Analyse eines Zugriffsdatensatzes 6 nicht nur festgestellt werden kann, dass dieser von einem vertrauenswürdigen Schlüsselmechanismus ausgestellt wurde sondern von welchem konkreten Schlüsselmechanismus 3 ein konkreter Zugriffsdatensatz 6 ausgestellt wurde. Diese Zugriffsdatensätze 6 sind des Weiteren mit einem digitalen Schlüssel 4 signiert, welcher dem Schlüsselmechanismus bekannt ist. Die Signatur signiert vorteilhafter Weise den gesamten Inhalt des Schlüsselmechanismus 6 (außer der Signatur selbst), kann jedoch in konkreten Implementierungen auch nur Teile des Zugriffsdatensatzes 6 umfassen. Insbesondere kann in bestimmten Implementierungen auf die Signatur der Identität des Servers 9 verzichtet werden, sodass diese z.B. bei der Weiterleitung des Zugriffsdatensatzes 6 in komplexen Netzwerken 8 (z.B. über Reverse-Proxy-Server) ersetzt werden kann. Die Signatur muss jedoch zumindest jenen Teil des Zugriffsdatensatzes 6 umfassen, der später genutzt wird um die zeitliche Nähe der Ausstellung des Zugriffsdatensatzes 6 zum Zeitpunkt der Überprüfung festzustellen. Je nach Beschaffenheit der Signatur kann diese ggf. implizit die Identität des Schlüsselmechanismus 3 enthalten. Die Signatur erfolgt mit einem geeigneten kryptografischen Verfahren. Es sind grundsätzlich sowohl asymmetrische als auch symmetrische Verfahren geeignet wobei bei symmetrischen Verfahren (z.B. AES

009:13

in Kombination mit SHA1) die Schlüssel 4 und 10 identisch sind und möglichst nur dem Schlüsselmechanismus 3 sowie dem Server 9 bekannt sein sollten während bei asymmetrischen Verfahren (z.B. Digital Signature Algorithm, DSA) der private Schlüssel 4 nur dem Schlüsselmechanismus bekannt sein sollte während die Geheimhaltung des öffentlichen Schlüssels 10 nicht notwendig ist.

Der Zugriffsdatensatz kann vorteilhafter Weise in Form einer URL erstellt werden, da solche URLs einen weit verbreiteten Standard darstellen, und diese URLs von vielen unterschiedlichen Arten von mobilen Endgeräten verarbeitet werden können. Der Aufbau einer solchen URL könnte z.B. wie folgt sein:

```
https://examplerestaurant.org/table1?t=2012-07-03T182210&tagid=123&sig=xxxxxxxxxxx
```

In diesem Fall repräsentiert der Teil „https://examplerestaurant.org/table1“ den zu kontaktierenden Server 9 sowie die geschützte Ressource 11. Der Teil „t=2012-07-03T182210“ repräsentiert den Zeitpunkt der Ausstellung des Zutrittsdatensatzes. Der Teil „tagid=123“ repräsentiert optionale zusätzliche Daten, die im Autorisierungsdatensatz 6 enthalten sein können, z.B. die Identität des Schlüsselmechanismus 3. Der Teil „sig=xxxxxxxxxxx“ repräsentiert die Signatur, welche vom Schlüsselmechanismus 3 mit Hilfe des Schlüssels 4 erstellt wird und mit welcher Signatur die restlichen Teile der URL signiert werden, sodass der Server 9 mit Hilfe des eigenen Schlüssels 10 überprüfen kann, dass die Daten im Zugriffsdatensatz 6 von einem vertrauenswürdigen Schlüsselmechanismus 3 ausgestellt und danach nicht manipuliert wurden.

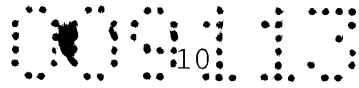
Der Zugriffsdatensatz 6 wird vom Schlüsselmechanismus 3 über eine lokal begrenzte Datenverbindung 7 zum mobilen Endgerät 2 übertragen. Diese Übertragung kann über eine Vielzahl unterschiedlicher Arten von Datenverbindungen 7 erfolgen. Es ist dabei lediglich erforderlich, dass über die Datenverbindung 7 Daten vom Schlüsselmechanismus 3 zum mobilen Endgerät 2 übertragen werden können, die Übertragung von Daten in entgegengesetzter Richtung ist vorteilhaft, jedoch nicht zwingend notwendig. Die lokale Begrenztheit der Datenverbindung ist notwendig, damit davon ausgegangen werden kann, dass ein mobiles Endgerät, welches Daten über diese lokale Datenverbindung empfangen kann, sich in dessen lokaler Nähe befindet. Wie stark diese lokale Begrenzung ausgeprägt sein muss hängt vom jeweiligen Anwendungsfall ab. Speziell die NFC Technologie ist darauf ausgelegt, die Kommunikation der beteiligten Geräte auf eine Distanz von wenigen Zentimetern begrenzen zu können. Andere denkbare Technologien wie WLAN erlauben die Kommunikation über eine deutlich größere Distanz mit einer weniger scharfen lokalen Begrenzung. Auch eine vom Betreiber einer solchen Vorrichtung ungewünschte Erweiterung der Distanz, über die ein mobiles Endgerät 2 Zugriffsdatensätze 6 empfangen kann, wäre bei Technologien wie WLAN deutlich einfacher, wodurch die Zuverlässigkeit des Verfahrens abnehmen würde. Es liegt an der jeweiligen Anwendung, welche konkreten Technologien für die lokal begrenzte Datenverbindung 7 in Frage kommen und es liegt an der jeweiligen Implementierung, sicherzustellen, dass die lokale Begrenztheit der Datenverbindung den jeweiligen Anforderungen entspricht.

Vorteilhafter Weise kann der Schlüsselmechanismus 3 die lokale Nähe eines mobilen Endgerätes 2 feststellen, sowie dessen Wunsch, einen Zugriffsdatensatz 6 zu empfangen. In einem solchen Fall erstellt der Schlüsselmechanismus 3 genau dann einen Zugriffsdatensatz 6, wenn ein solcher von einem mobilen

009:13

Endgerät 2 benötigt wird. Beispiele für diese Art lokaler Datenverbindungen sind NFC und Bluetooth. Sollte für die lokale Datenverbindung NFC verwendet werden, kann der Schlüsselmechanismus 3 z.B. eine ISO 14443 Karte emulieren (ISO 14443 card emulation mode) und den Zugriffsdatensatz 6 in Form einer URL über eine Standard NDEF Nachricht versenden, wodurch eine hohe Kompatibilität mit vielen existierenden mobilen Endgeräten gewährleistet werden kann.

Verfügt der Schlüsselmechanismus 3 über keine Möglichkeit, die lokale Nähe eines mobilen Endgerätes 2 bzw. dessen Wunsch, einen Zugriffsdatensatz zu empfangen, festzustellen, so erstellt der Schlüsselmechanismus 3 fortlaufend neue Zugriffsdatensätze 6 und versendet diese an potentiell in der Nähe befindliche mobile Endgeräte 2. Ein Beispiel für diese Art lokaler Datenverbindungen 7 wäre die Übertragung in Form eines Barcodes, welcher vom Schlüsselmechanismus 3 erstellt und über ein am Schlüsselmechanismus 3 befindliches Display angezeigt wird. In diesem Fall würde das mobile Endgerät 2 den Zugriffsdatensatz 6 empfangen, indem der Barcode über eine im mobilen Endgerät 2 befindliche Kamera gelesen und entschlüsselt wird. Nach dem Empfang des Zugriffsdatensatzes 6 durch das mobile Endgerät 2 wird dieser vom mobilen Endgerät 2 verarbeitet. Vorteilhafter Weise veranlasst das mobile Endgerät 2 in weiterer Folge automatisch den weiteren Ablauf des Verfahrens und somit den Zugriff auf die im Zugriffsdatensatz 6 identifizierte Ressource 11. Ist der Zugriffsdatensatz 6 beispielsweise als URL ausgebildet, kann die automatische Verarbeitung am mobilen Endgerät 2 in der Form erfolgen, dass darauf ein Webbrowser gestartet und darin die URL geöffnet wird. Alternativ kann für die Verarbeitung des Zugriffsdatensatzes 6 eine Interaktion zwischen dem Benutzer 1 und dem mobilen Endgerät 2 eingebaut werden, z.B. indem der Benutzer 1 um eine Freigabe gefragt wird, bevor der Zugriff auf den Server 9 bzw. Ressource 11 erfolgt. Ein



Benutzer 1 könnte auch zur Installation einer bestimmten, für die Verarbeitung des Zugriffsdatensatzes 6 notwendigen Software (App) aufgefordert werden.

In weiterer Folge überträgt das mobile Endgerät 2 den Zugriffsdatensatz 6 über ein Netzwerk 8 zum Server 9. Im Beispiel eines Zugriffsdatensatzes 6 der als URL ausgeprägt wäre und über einen am mobilen Endgerät 2 installierten Web-Browser geöffnet würde, würde die Übertragung des Zugriffsdatensatzes 6 (der URL) in Form eines durch den Browser initiierten http bzw. https Requests realisiert.

Der Server 9 verfügt selbst über einen Schlüssel 10, der zum Schlüssel 4 des Schließmechanismus 3 passt, welcher Schlüssel 4 für die Signatur des Zugriffsdatensatzes 6 verwendet wurde. Mit Hilfe dieses Schlüssels 10 und geeigneter kryptografischer Verfahren stellt der Server 9 die Gültigkeit der Signatur des Zugriffsdatensatzes 6 fest.

Des Weiteren ist der Server 9 in der Lage, die zeitliche Nähe der Ausstellung des Zugriffsdatensatzes 6 festzustellen. Je nach konkreter Ausbildung des Zugriffsdatensatzes 6 kann dies beispielsweise dadurch erfolgen, dass der Server 9 den im Zugriffsdatensatz 6 enthaltenen Zeitpunkt der Ausstellung desselben ausliest und anhand einer im Server 9 vorhandenen Uhr feststellt, ob der zeitliche Abstand zur Ausstellung des Schlüsseldatensatzes 6 innerhalb vorgegebener Grenzen liegt. Ist sowohl die Gültigkeit der Signatur als auch die zeitliche Nähe zum Zeitpunkt der Ausstellung des Zugriffsdatensatzes 6 gegeben, gewährt der Server 9 den Zugriff auf die geschützte Ressource 11 durch das mobile Endgerät 2.

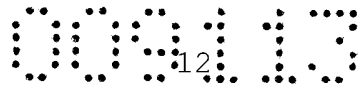
Der Server 9 muss die Überprüfung des Zugriffsdatensatzes 6 nicht zwingendermaßen selbst ausführen sondern kann diese auch an eine weitere Instanz delegieren. Insgesamt sind für die

Implementierung des Servers 9 sowie die Auslieferung der Ressource 11 verschiedene Techniken denkbar, wie sie heute z.B. in Web-Servern eingesetzt werden, einschließlich der Delegation von Teilaufgaben an andere Systeme, sofern die zuvor genannten Bedingungen erfüllt werden.

Bei der geschützten Ressource 11 kann es sich um verschiedenste Arten von Ressourcen handeln, z.B. um einzelne Dateien wie Bilddateien oder um ganze Websites auf denen in weiterer Folge weitere Interaktionen durchgeführt werden. Es ist auch denkbar, das Verfahren bzw. die Vorrichtung mit weiteren Authentifizierungsmechanismen, z.B. mit Benutzername und Passwort zu kombinieren. Auf diese Weise ist z.B. die Nutzung im Rahmen einer Mehr-Faktor-Authentifizierung möglich.

Sollte die Vorrichtung bzw. das Verfahren nicht zum Zugriff auf eine einzelne Datei sondern auf mehrere Dateien bzw. eine weiterführende Interaktion verwendet werden, so sind zum Vorhalten des Authentifizierungsergebnisses bekannte Verfahren anwendbar. Im Falle der Nutzung mit einem Web-Server kann das Authentifizierungsergebnis z.B. in Form eines HTTP-Cookies gespeichert werden.

Fig. 2 zeigt ein schematisches Ablaufdiagramm eines erfindungsgemäßen Verfahrens. Im Diagramm ist die Variante illustriert, in der der Schlüsselmechanismus in Schritt a1 fortlaufend neue Zugriffsschlüssel 6 erstellt, ohne die lokale Nähe eines mobilen Endgerätes 2 zu berücksichtigen. Der Schlüsselmechanismus 3 erstellt in Schritt a1 mit Hilfe seines Schlüssels 4 und mit Hilfe eines Zeitgebers 5, fortlaufend, in festgelegten Abständen, neue Zugriffsdatensätze 6 und versendet diese über eine lokal begrenzte Datenverbindung 7 an potentiell in der Nähe befindliche mobile Endgeräte. Die Häufigkeit der Erstellung neuer Zugriffsdatensätze 6 wird



dabei idealer Weise so gewählt, dass ein neuer Zugriffsdatensatz spätestens dann erstellt wird, wenn der zuvor erstellte Zugriffsdatensatz ein Alter erreicht hat, das dazu führt, dass er vom Server 9 nicht mehr als gültig akzeptiert wird.

Ein Benutzer 1 bringt sein mobiles Endgerät 2 in Schritt a2 in die lokale Nähe des Schlüsselmechanismus 3. Das mobile Endgerät 2 empfängt in Schritt a3 über die lokale Datenverbindung 7 den Zugriffsdatensatz 6. Das mobile Endgerät 2 verarbeitet diesen und sendet ihn in Schritt a4 über ein Netzwerk 8 weiter an den Server 9. Dieser Server 9 überprüft in Schritt a5 den Zugriffsdatensatz 6 anhand des eigenen Schlüssels 10 und der aktuellen Uhrzeit auf Gültigkeit. Ist diese Gültigkeit gegeben, sendet er in Schritt a6 die gewünschte Ressource zurück an das mobile Endgerät 2, welches diese in Schritt a7 verarbeitet, z.B. dem Benutzer präsentiert. Die Rückgabe der konkreten Ressource in Schritt a6 muss dabei nicht unmittelbar erfolgen sondern kann anhand bekannter Techniken auch indirekt erfolgen, z.B. indem der Server 9 an das mobile Endgerät lediglich das Autorisierungsergebnis und eine Umleitung auf die eigentliche Ressource zurücksendet.

In den Schritten a8 kann das Autorisierungsergebnis potentiell für eine fortlaufende Kommunikation verwendet werden.

Patentansprüche:

1. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) über ein Netzwerk (8) und einen Server (9), wobei die Identitäten der Ressource (11) und des Servers (9) in einem Zugriffsdatensatz (6) enthalten sind, der von einem Schlüsselmechanismus (3) erstellt wird und über eine lokal begrenzte Datenverbindung (7) an das mobile Endgerät (2) gesendet wird, welches mobile Endgerät (2) über Mittel zur Herstellung einer Verbindung mit einem Netzwerk (8) aufweist und den Zugriffsdatensatz (6) über dieses Netzwerk (8) an einen Server (9) sendet, welcher Server (9) anhand des Zugriffsdatensatzes (6) den Zugriff auf die Ressource (11) steuert, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) den Zugriffsdatensatz (6) mit Hilfe eines Zeitgebers (5) derart erstellt, dass der Server (9) ermitteln kann, ob der Zugriffsdatensatz (6) in zeitlicher Nähe zum Zeitpunktes des Zugriffs auf die Ressource (11) durch das mobile Endgerät (2) erfolgt ist und der Server (9) diesen Umstand überprüft und den Zugriff nur dann ermöglicht, wenn diese Voraussetzung gegeben ist.
2. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach Anspruch 1, dadurch gekennzeichnet, dass der Zugriffsdatensatz (6) vom Schlüsselmechanismus (3) mit Hilfe eines ihm zur Verfügung stehenden Schlüssels (4) und geeigneter kryptografischer Verfahren derart signiert wird, dass der Server (9) mit Hilfe eines ihm zur Verfügung stehenden Schlüssels (10) und geeigneter kryptografischer Verfahren feststellen kann, dass der Zugriffsdatensatz von einem

vertrauenswürdigen Schlüsselmechanismus ausgestellt wurde und nach dessen Ausstellung nicht in unerlaubter Weise manipuliert wurde und dieser Server (9) den Zugriff auf die Ressource (11) nur dann ermöglicht, wenn diese Voraussetzungen gegeben sind.

3. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Zugriff auf die Ressource (11) durch ein Smartphone, einen Rechner, einen Tablet-Computer oder dgl. erfolgt.
4. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass für die Übertragen des Zugriffsdatensatzes (6) vom Schlüsselmechanismus (3) zum mobilen Endgerät (2) zwischen diesen eine Nahfeld-Kommunikations- (NFC)-Verbindung, eine Hochfrequenzverbindung oder eine Bluetooth-Verbindung als lokale Datenverbindung aufgebaut wird.
5. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Zugriffsdatensatz (6) die Form eines einheitlichen Quellenanzeigers (Uniform Resource Locator, URL) aufweist.
6. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass zwischen mobilem Endgerät (2) und Server (9) eine Verbindung über das Internet aufgebaut wird.
7. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 6,

dadurch gekennzeichnet, dass für den Zugriff auf die Ressource (11) durch das mobile Endgerät (2) neben der Vorbereitung des mobilen Endgerätes (2) zur Teilnahme am gegenständlichen Verfahren sowie die Bringung des mobilen Endgerätes (2) in die lokale Nähe des Schlüsselmechanismus (3) keine weitere Benutzerinteraktion notwendig ist, insbesondere keine zusätzlichen Authentifizierungsschritte, wie die Eingabe eines Kennwortes.

8. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass der Schlüssel (4) und der Schlüssel (10) identisch sind und für die Signatur des Zugriffsdatensatzes (6) ein symmetrisches kryptografisches Verfahren zum Einsatz kommt.
9. Verfahren zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass es sich beim Schlüssel (4) und einen privaten Schlüssel des Schlüsselmechanismus handelt und bei Schlüssel (10) um einen dazu passenden öffentlichen Schlüssel handelt und für die Signatur des Zugriffsdatensatzes (6) ein asymmetrisches kryptografisches Verfahren zum Einsatz kommt.
10. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) welches Mittel zum Empfang von Daten über eine lokal begrenzte Datenverbindung (7) sowie Mittel zur Herstellung einer Verbindung mit einem Netzwerk (8) aufweist und ausgebildet ist, über die lokale Datenverbindung (7) einen Zugriffsdatensatz (6) von einem Schlüsselmechanismus (3), zu empfangen, welcher

Zugriffsdatensatz (6) verwendet werden kann, über einen Server (9) auf eine Ressource (11) zuzugreifen, wobei der Schlüsselmechanismus (3) ausgebildet ist, Zugriffsdatensätze (6) zu erstellen, welche einen bestimmten Server (9) und eine bestimmte Ressource (11) identifizieren und über eine lokal begrenzte Datenverbindung (7) an ein mobiles Endgerät (2) zu versenden und wobei der Server (9) ausgebildet ist, Zugriffsdatensätze (6) über ein Netzwerk (8) mit welchem er verbindbar ist, zu empfangen und anhand dieser Zugriffsdatensätze (6) den Zugriff auf eine Ressource (11) zu steuern, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) ausgebildet ist, mit Hilfe eines Zeitgebers (5) die erstellten Zugriffsdatensätze (6) so zu gestalten, dass der Server (9) bei Prüfung eines Zugriffsdatensatzes (6) feststellen kann, ob dieser Zugriffsdatensatz (6) in zeitlicher Nähe zu dieser Feststellung ausgestellt wurde und der Server (9) ausgebildet ist, diesen Umstand zu überprüfen und den Zugriff nur dann zu ermöglichen, wenn diese Voraussetzung gegeben ist.

11. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach Anspruch 10, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) ausgebildet ist, den Zugriffsdatensatz (6) mit Hilfe eines dem Schlüsselmechanismus (3) zur Verfügung stehenden Schlüssels (4) und geeigneter kryptografischer Verfahren derart zu signieren, dass der Server (9) mit Hilfe eines ihm zur Verfügung stehenden Schlüssels (10) und geeigneter kryptografischer Verfahren feststellen kann, ob der Zugriffsdatensatz von einem vertrauenswürdigen Schlüsselmechanismus ausgestellt und nach dessen Ausstellung nicht in unerlaubter Weise manipuliert wurde und dieser Server (9) ausgebildet ist,

diese Überprüfung durchzuführen und den Zugriff auf die Ressource (11) nur dann zu ermöglichen, wenn diese Voraussetzungen gegeben sind.

12. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 11, dadurch gekennzeichnet, dass die Mittel zur Herstellung der lokalen Datenverbindung (7) durch einen Nahfeldkommunikations- (NFC)-Sender und Empfänger, RFID-Transponder und/oder Bluetooth-Sender und Empfänger gebildet ist.
13. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, dass das mobile Endgerät (2) über eine grafische Benutzerschnittstelle verfügt.
14. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, dass das mobile Endgerät (2) durch ein Smartphone, einen Rechner, einen Tablet-Computer oder dgl. gebildet ist.
15. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) ausgebildet ist, Zugriffsdatensätze (6) in Form einheitlicher Quellenanzeiger (Uniform Resource Locator, URL) zu erstellen und das mobile Endgerät (2) sowie der Server (9) ausgebildet sind, solche Zugriffsdatensätze zu verarbeiten.
16. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, dass das Netzwerk (8) durch

das Internet und der Server (9) durch einen Webserver gebildet sind.

17. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) als Gerät gebildet ist, das außer der Schnittstelle für die lokale Datenverbindung (7) keine weitere elektronische Benutzerschnittstelle aufweist, insbesondere keine grafische Anzeige und keine Tasten aufweist.
18. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 17, dadurch gekennzeichnet, dass das mobile Endgerät (2) ausgebildet ist, Zugriffsdatensätze (6) nach deren Empfang automatisch, ohne weitere Benutzerinteraktion zu verarbeiten.
19. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 18, dadurch gekennzeichnet, dass der Server (9) ausgebildet ist, den Zugriff auf eine Ressource (11) anhand der Daten im Zugriffsdatensatz (6) zu steuern, ohne zusätzliche Authentifizierungsdaten wie z.B. ein Kennwort, zu erfordern.
20. Vorrichtung zum Zugriff auf eine Ressource (11) durch ein mobiles Endgerät (2) nach einem der Ansprüche 10 bis 19, dadurch gekennzeichnet, dass der Schlüsselmechanismus (3) ausgebildet ist, den Zugriffsdatensatz (6) mit Hilfe eines asymmetrischen kryptografischen Verfahrens zu signieren und es sich beim dafür verwendeten Schlüssel (4) um einen privaten Schlüssel des Schlüsselmechanismus (3) handelt und dass der Server (9) ausgebildet ist, den

009:13

Zugriffsdatensatz (6) anhand eines passenden asymmetrischen kryptografischen Verfahrens zu überprüfen und es sich beim dafür verwendete Schlüssel (10) um einen zum privaten Schlüssel (4) passenden öffentlichen Schlüssel handelt.

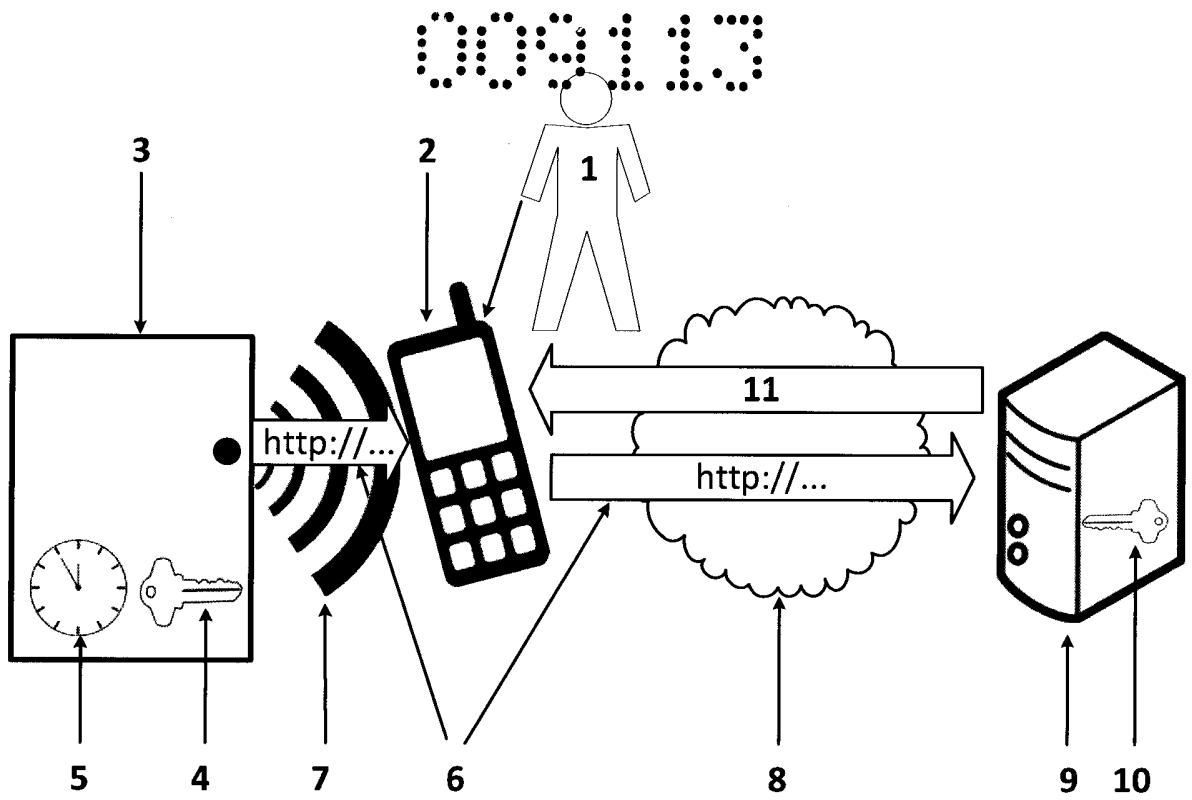


Fig. 1

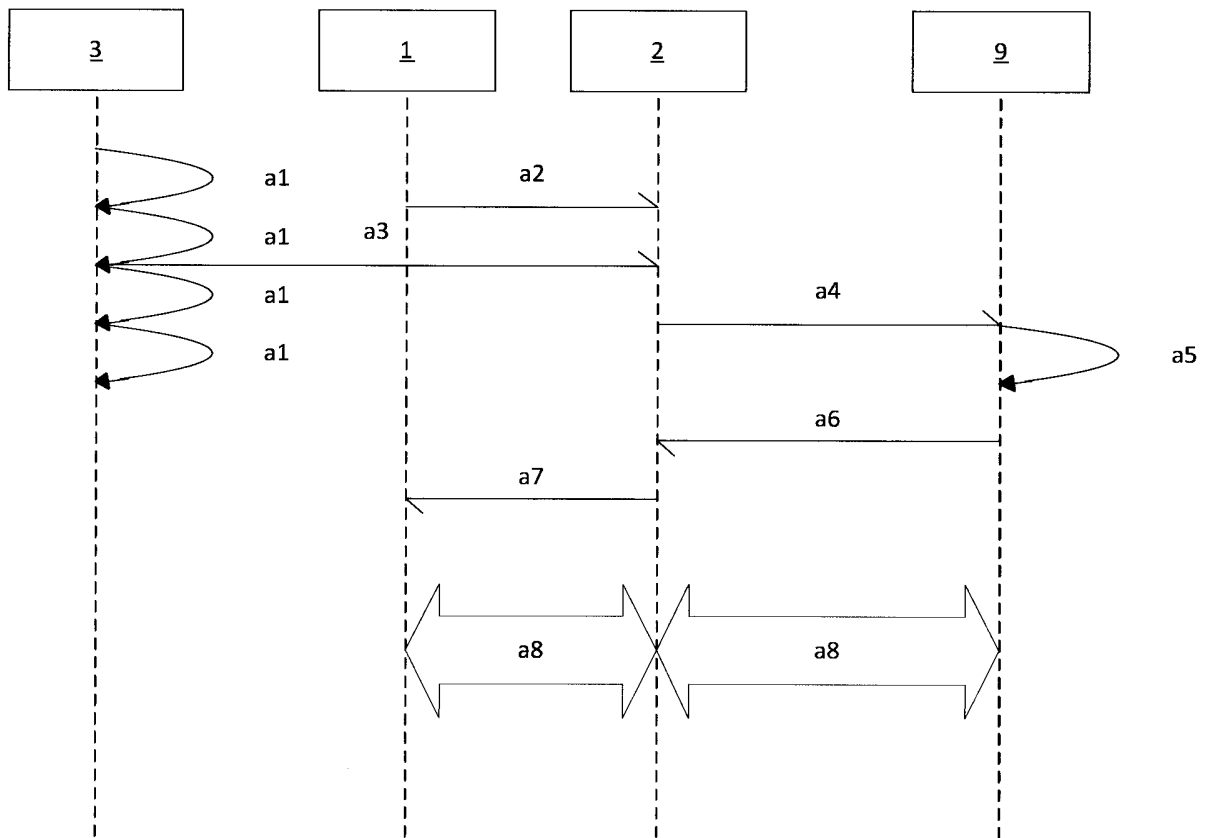


Fig. 2

Klassifikation des Anmeldungsgegenstands gemäß IPC:

H04W 12/06 (2009.01); **H04W 52/02** (2009.01); **H04L 9/32** (2006.01); **H04B 5/02** (2006.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:

H04W 12/06 (2013.01); **H04W 52/0258** (2013.01); **H04L 9/3297** (2013.01); **H04B 5/02** (2013.01);
H04L 63/04 (2013.01); **H04L 63/108** (2013.01)

Recherchierter Prüfstoff (Klassifikation):

H04W, H04L, H04B

Konsultierte Online-Datenbank:

WPI, EPODOC, IEEEExplore, ScienceDirect

Dieser Recherchenbericht wurde zu den am **27.09.2012** eingereichten Ansprüchen **1–20** erstellt.

Kategorie ¹⁾	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2008182592 A1 (CHA et al.) 31. Juli 2008 (31.07.2008) Figuren; Zusammenfassung; Paragraphen 0013, 0056.	1–20
X	US 2011087887 A1 (LUFT et al.) 14. April 2011 (14.04.2011) Figuren; Zusammenfassung; Paragraphen 0017, 0045, 0046, 0064.	1–20

Datum der Beendigung der Recherche:

30.08.2013

Seite 1 von 1

Prüfer(in):

MESA PASCASIO Johannes

¹⁾ **Kategorien** der angeführten Dokumente:

X Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.

Y Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.

A Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.

P Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.

E Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).

& Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.