(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 207 033 B4** 2022.03.24

(12) # Patentschrift

(21) Aktenzeichen: **10 2020 207 033.4**
(22) Anmeldetag: **04.06.2020**
(43) Offenlegungstag: **09.12.2021**
(45) Veröffentlichungstag der Patenterteilung: **24.03.2022**

(51) Int Cl.: ***H04L 9/00*** (2022.01)
H04L 9/32 (2006.01)
H04L 12/22 (2006.01)
H04W 12/069 (2021.01)
H04W 84/12 (2009.01)
H04W 76/10 (2018.01)
G06F 21/44 (2013.01)
H04L 9/40 (2022.01)
H04L 41/08 (2022.01)
H04L 12/28 (2006.01)
D06F 34/05 (2020.01)
A47L 15/00 (2006.01)

(73) Patentinhaber:
BSH Hausgeräte GmbH, 81739 München, DE

(72) Erfinder:
Jahner, Matthias, Dr., 83329 Waging, DE; Söllner, Christoph, Dr., 81475 München, DE

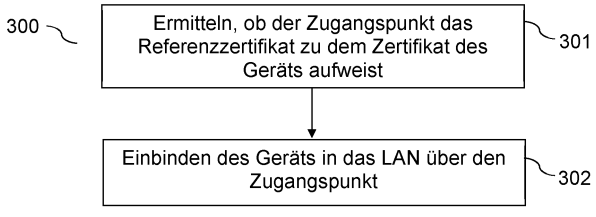
(56) Ermittelter Stand der Technik:

DE	**10 2004 034 363**	**A1**
DE	**10 2014 102 168**	**A1**
DE	**10 2017 214 359**	**A1**

Norm IEEE Std 802.11-2016. IEEE Standard for information technology -Telecommunications and information exchange between systems local and metropolitan area networks -Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. - ISBN 978-1-5044-3645-8. DOI: 10.1109/IEEESTD.2016.7786995. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7786995 [abgerufen am 19.06.2017]

(54) Bezeichnung: **Vorrichtungen und Verfahren zur Einbindung eines Geräts in ein Local Area Network**

(57) Zusammenfassung: Es wird ein Verfahren (300) zur Einbindung eines Geräts (130) in ein LAN (111) beschrieben, wobei das Gerät (130) ein Zertifikat (213) aufweist, das aus einem Geräte-Referenzzertifikat (211) abgeleitet wurde. Das Verfahren (300) umfasst das Überprüfen (301), ob das Zertifikat (13) des Geräts (130) zu zumindest einem Referenzzertifikat (201) passt, das an einem ersten Zugangspunkt (110) zu einem ersten LAN (111) verfügbar ist. Des Weiteren umfasst das Verfahren (300) das Einbinden (302) des Geräts (130) in das erste LAN (111), wenn ermittelt wird, dass das Zertifikat (213) des Geräts (130) zu zumindest einem an dem ersten Zugangspunkt (110) verfügbaren Referenzzertifikat (201) passt.



Beschreibung

[0001] Die Erfindung betrifft die effiziente, zuverlässige und komfortable Einbindung von einem Gerät, insbesondere einem Hausgerät, in ein Local Area Network (LAN).

[0002] Wenn ein Nutzer ein neues, LAN-fähiges, Gerät, insbesondere ein neues Hausgerät, zu sich nach Hause bringt, muss der Nutzer dieses Gerät typischerweise zunächst mit einem relativ hohen Zeitaufwand in sein LAN einbinden.

[0003] Aus der DE 10 2004 034 363 A1 ist ein Verfahren zur Steuerung des Zugriffs von mobilen Endgeräten auf Rechnernetzwerke vorbekannt. Dabei kommen Zertifikate zum Einsatz. Die DE 10 2014 102 168 A1 beschäftigt sich mit einem Verfahren zum Erstellen von Gerätezertifikaten für elektronische Geräte und erwähnt dabei insbesondere Zertifikatsketten. Die DE 10 2017 214 359 A1 offenbart sogenannte Herstellerzertifikate.

[0004] Das vorliegende Dokument befasst sich mit der technischen Aufgabe, eine besonders komfortable, zuverlässige und sichere Einbindung eines LAN-fähigen Geräts in ein LAN zu ermöglichen.

[0005] Die Aufgabe wird jeweils durch die Gegenstände der unabhängigen Patentansprüche gelöst. Vorteilhafte Ausführungsformen sind insbesondere in den abhängigen Patentansprüchen definiert, in nachfolgender Beschreibung beschrieben oder in der beigefügten Zeichnung dargestellt.

[0006] Gemäß einem Aspekt der Erfindung wird ein (ggf. Computer-implementiertes) Verfahren zur Einbindung eines Geräts in ein Local Area Network (LAN), insbesondere in ein Wireless LAN, beschrieben. Das Gerät kann insbesondere ein Hausgerät, etwa ein Ofen, ein Kühlschrank, ein Herd, eine Spülmaschine, eine Waschmaschine, ein Trockner, eine Küchenmaschine, eine Kaffeemaschine, etc., sein. Das Gerät kann ein Kommunikationsmodul umfassen, das ausgebildet ist, eine drahtgebundene und/oder eine drahtlose LAN Verbindung (insbesondere gemäß IEEE 802.11) zu einem Zugangspunkt (auf Englisch Access Point) aufzubauen. Das Verfahren kann durch einen (ersten) Zugangspunkt ausgeführt werden.

[0007] Das Gerät weist ein Zertifikat auf, das aus einem Geräte-Referenzzertifikat abgeleitet wurde. Das Zertifikat kann dabei entlang einer Geräte-Zertifikatskette über ein oder mehrere Zwischenzertifikate aus dem Geräte-Referenzzertifikat hergeleitet worden sein. Dabei kann das Geräte-Referenzzertifikat einer bestimmten Entität (z.B. dem Hersteller des Geräts) zugeordnet sein. Es können dann aus dem Geräte-Referenzzertifikat für unterschiedliche Geräte der Entität unterschiedliche Zertifikate generiert und auf dem jeweiligen Gerät bereitgestellt werden. Dabei kann das Zertifikat jeweils auf einer Speichereinheit, insbesondere auf einem Trusted-Platform-Module (TPM) oder einer anderen als sicher bewerteten Speicherlösung, des jeweiligen Geräts gespeichert sein. Das Gerät kann ausgebildet sein, aus dem Zertifikat des Geräts die Geräte-Zertifikatskette zu ermitteln, und/oder das Gerät kann eingerichtet sein, die Geräte-Zertifikatskette ganz oder teilweise bereitzustellen. Die Geräte-Zertifikatskette kann z.B. auf dem Gerät gespeichert sein.

[0008] Das Referenzzertifikat einer Entität kann das Stammzertifikat der Entität oder ein von dem Stammzertifikat der Entität abgeleitetes Zertifikat sein. Unter dem Betriff „Geräte-Referenzzertifikat“ eines Geräts wird in diesem Dokument das Referenzzertifikat einer Entität verstanden, aus dem das Zertifikat des Geräts (d.h. das Zertifikat, das auf dem Gerät gespeichert ist und/oder das dem Gerät zugewiesen wurde) abgeleitet wurde. Bei dem Geräte-Referenzzertifikat handelt es sich somit um ein bestimmtes Referenzzertifikat einer bestimmten Entität (insbesondere der bestimmten Entität, der das Gerät zugeordnet ist).

[0009] Das Verfahren umfasst das Überprüfen, ob das Zertifikat des Geräts zu zumindest einem Referenzzertifikat passt, das an einem ersten Zugangspunkt zu einem ersten (W)LAN verfügbar ist. Insbesondere kann auf Basis des Zertifikats des Geräts überprüft werden, ob das Geräte-Referenzzertifikat (d.h. das Referenzzertifikat, aus dem das Zertifikat des Geräts abgeleitet wurde) an dem ersten Zugangspunkt verfügbar ist, insbesondere ob das Geräte-Referenzzertifikat auf einer Speichereinheit, etwa auf einem TPM oder einer anderen als sicher bewerteten Speicherlösung, des ersten Zugangspunkts gespeichert ist.

[0010] An dem ersten Zugangspunkt kann z.B. eine Liste mit ein oder mehreren Referenzzertifikaten (ggf. von unterschiedlichen Entitäten) verfügbar sein. Diese Liste kann z.B. bei der Herstellung des ersten Zugangspunkts in dem ersten Zugangspunkt bereitgestellt werden. Insbesondere kann die Liste mit einem oder mehreren Referenzzertifikaten auf einer Speichereinheit, insbesondere auf einem TPM, des ersten Zugangspunktes gespeichert sein. Es kann dann in effizienter und zuverlässiger Weise überprüft werden, ob das Geräte-Referenzzertifikat in der Liste mit ein oder mehreren Referenzzertifikaten enthalten ist oder nicht und/oder ob das Zertifikat des Geräts von einem der Referenzzertifikate in der Liste abgeleitet wurde (entlang einer Referenzkette).

[0011] Das Verfahren umfasst ferner das Einbinden des Geräts in das erste (W)LAN, wenn ermittelt wird, dass das Zertifikat des Geräts von zumindest einem an dem ersten Zugangspunkt verfügbaren Referenz-

zertifikat abgeleitet wurde. Das Einbinden des Geräts in das erste LAN kann erfolgen, wenn, insbesondere nur dann, wenn, bestimmt wird, dass das Geräte-Referenzzertifikat (d.h. das Referenzzertifikat, aus dem das Zertifikat des Geräts abgeleitet wurde) in der Liste mit ein oder mehreren Referenzzertifikaten enthalten ist, bzw. wenn, insbesondere nur dann, wenn, ermittelt wird, dass das Geräte-Referenzzertifikat an dem Zugangspunkt verfügbar ist, bzw. wenn, insbesondere nur dann, wenn ermittelt wird, dass das Zertifikat des Geräts von einem an dem ersten Zugangspunkt verfügbaren Referenzzertifikat abgeleitet wurde (und im Sinne der Informationssicherheit gültig).

[0012] Das Verfahren ermöglicht es, ein Gerät in effizienter, komfortabler und sicherer Weise in ein (W)LAN einzubinden. Die Einbindung kann dabei automatisch erfolgen, ohne dass Zugangsdaten (wie z.B. ein Pre-Shared-Key (PSK)) zu dem LAN von einem Nutzer eingegeben werden müssen. Die Einbindung kann z.B. automatisch bei Inbetriebnahme des Geräts erfolgen.

[0013] Das Verfahren kann umfassen, das Ermitteln von ein oder mehreren Netzwerkeinheiten, für die eine Zugriffsberechtigung des Geräts über das erste LAN vorliegt. Die ein oder mehreren Netzwerkeinheiten können dabei in einem Wide Area Network (WAN) außerhalb des ersten LAN (z.B. im Internet) angeordnet sein. Die ein oder mehreren Netzwerkeinheiten können in der auf dem ersten Zugangspunkt gespeicherten Liste aufgeführt sein. Die ein oder mehreren Netzwerkeinheiten können von der Entität betrieben bzw. bereitgestellt werden, der das Geräte-Referenzzertifikat zugeordnet ist.

[0014] Die Einbindung des Geräts in das erste LAN kann auf den Zugriff zu den ein oder mehreren Netzwerkeinheiten beschränkt sein. Insbesondere kann durch den ersten Zugangspunkt bewirkt werden, dass das Gerät nur auf die ein oder mehreren Netzwerkeinheiten zugreifen kann, und ansonsten keinen weiteren Zugriff auf Komponenten des ersten LAN oder auf andere Komponente des WAN aufweist. So kann die Sicherheit der (automatischen) Einbindung des Geräts weiter erhöht werden.

[0015] Das Verfahren kann umfassen, das Bereitstellen einer Kommunikationsverbindung zwischen dem Gerät und den ein oder mehreren Netzwerkeinheiten über den ersten Zugangspunkt, insbesondere über einen Router des ersten Zugangspunktes. Die Kommunikationsverbindung kann dann z.B. zur Fernwartung des Geräts genutzt werden (ausgehend von den ein oder mehreren Netzwerkeinheiten). Es kann somit einem Hersteller von Geräten ermöglicht werden, in effizienter und zuverlässiger Weise auf Geräte zuzugreifen (da sich die Geräte automatisch mit den ein oder mehreren Netzwerkeinheiten (z.B. Servern) des Herstellers verbinden).

[0016] Wie bereits oben dargelegt, kann an dem ersten Zugangspunkt eine Liste mit ein oder mehreren Referenzzertifikaten verfügbar, insbesondere gespeichert, sein. Die Liste kann für jedes der Referenzzertifikate (und für jede damit assoziierte Entität) jeweils zumindest eine Netzwerkeinheit anzeigen, für die Geräte, die ein zu dem jeweiligen Referenzzertifikat passendes Zertifikat aufweisen, eine Zugriffsberechtigung aufweisen. So kann es unterschiedlichen Entitäten in effizienter und sicherer Weise ermöglicht werden, auf die Geräte der jeweiligen Entität zuzugreifen.

[0017] Das Verfahren kann umfassen, das Ermitteln der Geräte-Zertifikatskette zwischen dem Zertifikat des Geräts und dem Geräte-Referenzzertifikat, wobei die Geräte-Zertifikatskette ein oder mehrere Zwischenzertifikate zwischen dem Zertifikat des Geräts und dem Geräte-Referenzzertifikat anzeigt. Die Geräte-Zertifikatskette kann ganz oder teilweise z.B. von dem Gerät an den ersten Zugangspunkt gesendet und von dem ersten Zugangspunkt empfangen werden. Es kann dann in besonders effizienter und präziser Weise auf Basis der Geräte-Zertifikatskette überprüft werden, ob das Zertifikat des Geräts zu zumindest einem Referenzzertifikat passt, das an dem ersten Zugangspunkt zu dem ersten LAN verfügbar ist.

[0018] Der erste Zugangspunkt kann ggf. ein beliebiger Zugangspunkt sein, in dessen Empfangsbereich sich das Gerät befindet. Beispielsweise kann in einem urbanen Umfeld der erste Zugangspunkt von einem Nachbarn des Nutzers des Geräts betrieben werden. Durch den ersten Zugangspunkt kann ein erster (vorläufiger und/oder beschränkter) Zugang zu einem LAN und darüber zu einem WAN ermöglicht werden. Für einen vollständigen Zugang zu einem LAN und/oder zu einem WAN kann es erforderlich sein, dass das Gerät (automatisch) mit einem zweiten Zugangspunkt verbunden wird (z.B. mit einem Zugangspunkt des Nutzers).

[0019] Das Verfahren umfasst, das Ermitteln von zumindest einer Netzwerkeinheit, für die eine Zugriffsberechtigung des Geräts über das erste LAN vorliegt. Dabei zeigt die Netzwerkeinheit zumindest einen zweiten Zugangspunkt zu einem zweiten LAN an. Diese Information kann z.B. in einem Nutzerkonto des Nutzers des Geräts auf der Netzwerkeinheit gespeichert sein. In dem Nutzerkonto können die Zugangsdaten zu dem zweiten Zugangspunkt gespeichert sein (z.B. der PSK zu dem zweiten Zugangspunkt).

[0020] Es wird dann eine Kommunikationsverbindung zwischen dem Gerät und der Netzwerkeinheit

über den ersten Zugangspunkt aufgebaut, um es dem Gerät zu ermöglichen, die Zugangsdaten zu dem zweiten Zugangspunkt von der Netzwerkeinheit zu beziehen. So kann dann ein automatisches „Umhängen“ des Geräts von dem ersten LAN zu einem zweiten LAN ermöglicht werden, insbesondere, um dem Gerät innerhalb des zweiten LANs einen ggf. uneingeschränkten Zugang zu einem LAN und/oder zu dem WAN (etwa dem Internet) zu ermöglichen. Durch das automatische Einbinden in ein zweites LAN kann der Komfort für den Nutzer weiter erhöht werden. Das Einbinden in das zweite LAN kann z.B. durchgeführt werden, um es dem Nutzer zu ermöglichen, das Geräts fernzusteuern (z.B. mit einem Anwendergerät, etwa einem Smartphone des Nutzers, das in das zweite LAN eingebunden ist).

[0021] Beispielsweise kann im Rahmen des Verfahrens überprüft werden, ob eine Fernsteuerung des Geräts durch ein Anwendergerät erfolgen soll. Es kann dann das LAN ermittelt werden, in das das Anwendergerät eingebunden ist. Insbesondere kann ermittelt werden, dass das Anwendergerät über den zweiten Zugangspunkt in das zweite LAN eingebunden ist. Es kann daraufhin automatisch veranlasst werden, dass das Gerät in das zweite LAN eingebunden wird, um eine Fernsteuerung des Geräts durch das Anwendergerät zu ermöglichen. Diese Verfahrensschritte können z.B. durch einen Zugangspunkt und/oder durch das Gerät ausgeführt werden.

[0022] Gemäß einem weiteren Aspekt der Erfindung wird ein (ggf. Computer-implementiertes) Verfahren zur Einbindung eines Geräts in ein LAN beschrieben. Das Verfahren kann durch das Gerät ausgeführt werden. Das Gerät weist dabei ein Zertifikat auf (z.B. auf einem TPM), das aus einem Geräte-Referenzzertifikat abgeleitet wurde.

[0023] Das Verfahren umfasst das Identifizieren eines ersten Zugangspunkts für ein erstes LAN, an dem ein Referenzzertifikat verfügbar ist, das zu dem Zertifikat des Geräts passt, insbesondere das dem Geräte-Referenzzertifikat entspricht. Mit anderen Worten, es kann nach einem geeigneten ersten Zugangspunkt gesucht werden, der das passende Referenzzertifikat aufweist. Die Suche nach einem geeigneten ersten Zugangspunkt kann dabei automatisch von dem Gerät initiiert werden (ohne Nutzerinteraktion), z.B. bei der ersten Inbetriebnahme des Geräts.

[0024] Des Weiteren umfasst das Verfahren das Einbinden des Geräts in das erste LAN über den ersten Zugangspunkt. Zu diesem Zweck kann sich das Gerät mit dem ersten Zugangspunkt verbinden. Es kann dann von dem Zugangspunkt ein (ggf. beschränkter) Zugang zu dem ersten LAN und/oder zu dem WAN ermöglicht werden. So kann ein komfortabler und sicherer Zugang des Geräts zu einem LAN und/oder zu einem WAN ermöglicht werden.

[0025] Das Verfahren umfasst das Zugreifen auf eine Netzwerkeinheit über den ersten Zugangspunkt. Dabei zeigt die Netzwerkeinheit (wie bereits oben dargelegt) zumindest einen zweiten Zugangspunkt zu einem zweiten LAN an. Es werden dann Zugangsdaten (z.B. ein PSK) zu dem zweiten Zugangspunkt von der Netzwerkeinheit bezogen.

[0026] Das Gerät kann dann (automatisch) unter Verwendung der Zugangsdaten zu dem zweiten Zugangspunkt über den zweiten Zugangspunkt in das zweite LAN (und über den zweiten Zugangspunkt in das WAN) eingebunden werden. Andererseits kann das Gerät (automatisch) von dem ersten Zugangspunkt abgemeldet werden. So kann in besonders komfortabler und sicherer Weise ein (ggf. vollwertiger) Zugang zu einem zweiten LAN (z.B. zu dem LAN des Nutzers) und darüber zu dem WAN ermöglicht werden.

[0027] Das Verfahren kann umfassen, das Aufbauen einer Kommunikationsverbindung zu einer Netzwerkeinheit über den ersten Zugangspunkt. Des Weiteren kann das Verfahren umfassen, das Bewirken einer Wartungsmaßnahme des Geräts durch Zugriff der Netzwerkeinheit auf das Gerät über den ersten Zugangspunkt. Es kann somit einer Entität (z.B. dem Hersteller des Geräts) ermöglicht werden, in effizienter und sicherer Weise Wartungsmaßnahmen durchzuführen.

[0028] Ein Zugangspunkt (d.h. eine Vorrichtung) zu einem LAN, der im Rahmen der Erfindung verwendet werden kann, ist eingerichtet, zu überprüfen, ob ein Zertifikat eines Geräts, das in das LAN eingebunden werden soll, zu einem Referenzzertifikat passt, das an dem Zugangspunkt verfügbar ist. Der Zugangspunkt ist ferner eingerichtet, das Gerät in das LAN einzubinden, wenn ermittelt wird, dass das Zertifikat des Geräts zu einem an dem Zugangspunkt verfügbaren Referenzzertifikat passt. Des Weiteren kann der Zugangspunkt eingerichtet sein, zumindest einen beschränkten Zugang zu einem WAN zu ermöglichen (z.B. auf eine beschränkte Liste von Netzwerkeinheiten (etwa Server und/oder URLs (Uniform Resource Locator)).

[0029] Die Ressourcen, die ein Gerät mit einem bestimmten Zertifikat einer Entität in dem LAN und/oder in dem WAN nutzen darf (etwa eine Verbindung mit ein oder mehreren bestimmten Parametern wie IP-Adressen, URLs, Protokollvarianten, Portnummern und dergleichen) können auf dem Zugangspunkt und/oder auf weiteren Routing-Komponenten des LANs fest mit einem jeweiligen Referenzzertifikat verknüpft sein. Damit kann automatisiert eine

Beschränkung des Zugangs basierend auf der Zugehörigkeit des Geräts zu einer Entität vorgenommen werden. Beispielsweise kann ein Hausgerät ausschließlich berechtigt werden, mit nur einem einzelnen Server im Internet, z.B. dem Backend des Herstellers des Hausgeräts, eine Verbindung aufzubauen.

[0030] In einer geeigneten Benutzerschnittstelle kann einem Nutzer oder einem Netzwerkadministrator eine Übersicht dargestellt werden, welche Referenzzertifikate auf einem Zugangspunkt zur Verfügung stehen. Des Weiteren können in dieser Darstellung die jeweils verknüpften Berechtigungen (URLs, Server, Protokollvarianten und dergleichen) angezeigt werden.

[0031] Dem Nutzer oder Administrator kann über die Nutzerschnittstelle die Möglichkeit gegeben werden, bestimmte Referenzzertifikate (von bestimmten Entitäten) herunterzuladen, zu installieren, zu löschen, zu aktivieren und/oder zu deaktivieren. Mit der Deaktivierung bzw. Entfernung eines Referenzzertifikats erlischt typischerweise unverzüglich jegliche Berechtigung aller aktuell mit dem Zugangspunkt verbundener Geräte (die dem gelöschten Referenzzertifikat zugeordnet sind). Insbesondere kann für diese Geräte die Verbindung zum LAN unterbrochen werden.

[0032] Ein Gerät, das im Rahmen der Erfindung verwendet werden kann, weist ein Zertifikat auf, das aus einem Geräte-Referenzzertifikat abgeleitet wurde. Das Gerät ist eingerichtet, einen ersten Zugangspunkt für ein erstes LAN zu identifizieren, an dem ein Referenzzertifikat verfügbar ist, das zu dem Zertifikat des Geräts passt, insbesondere das dem Geräte-Referenzzertifikat entspricht. Das Gerät ist ferner eingerichtet, in Reaktion darauf, eine Einbindung in das erste LAN über den ersten Zugangspunkt zu bewirken.

[0033] Es ist zu beachten, dass jegliche Aspekte der in diesem Dokument beschriebenen Verfahren und Vorrichtungen in vielfältiger Weise miteinander kombiniert werden können. Insbesondere können die Merkmale der Patentansprüche in vielfältiger Weise miteinander kombiniert werden.

[0034] Im Weiteren wird die Erfindung anhand von in der beigefügten Zeichnung dargestellten Ausführungsbeispielen näher beschrieben. Dabei zeigen

Fig. 1 ein Blockdiagramm eines Systems zur Einbindung eines Geräts in ein LAN;

Fig. 2a eine beispielhafte Zertifikatliste;

Fig. 2b eine beispielhafte Zertifikatskette; und

Fig. 3a und **Fig. 3b** Ablaufdiagramme von beispielhaften Verfahren zur Einbindung eines Geräts in ein LAN.

[0035] Wie eingangs dargelegt, befasst sich das vorliegende Dokument mit der komfortablen, sicheren und zuverlässigen Einbindung eines Geräts, insbesondere eines Hausgeräts, in ein LAN. In diesem Zusammenhang zeigt **Fig. 1** ein beispielhaftes System 100 mit einem LAN-fähigen Gerät 130. Das System 100 umfasst einen ersten Zugangspunkt 110 (z.B. einen Router) zu einem ersten (W)LAN 111 und einen zweiten Zugangspunkt 120 (z.B. einen Router) zu einem zweiten (W)LAN 121. Das Gerät 130 kann ein Kommunikationsmodul 132 umfassen, das es ermöglicht, das Gerät 130 in das erste LAN 111 (für eine erste LAN-Verbindung 112) und/oder in das zweite LAN 121 (für eine zweite LAN-Verbindung 122) einzubinden. Des Weiteren kann das Gerät 130 ein Steuermodul 131 aufweisen, das ausgebildet ist, Aktionen des Geräts 130 zu steuern.

[0036] Die Zugangspunkte 110, 120 können eingerichtet sein, jeweils eine Kommunikationsverbindung 113, 123 zu einer Netzwerkeinheit 102 (z.B. mit einem Server, etwa in einer Cloud) in einem Wide Area Network, WAN, (z.B. dem Internet) aufzubauen. Die LANs 111, 121 können Wireless LANs (WLAN) umfassen, insbesondere sein.

[0037] In diesem Dokument wird ein Verfahren beschrieben, bei dem ein Netzwerkgerät 130 automatisch einen, ggf. vollwertigen, Netzwerkzugang und zumindest einen Zugang zu einer entfernten Netzwerkeinheit 102 (z.B. zu einer Netzwerkeinheit 102 eines Herstellers des Geräts 130) erhält. Ein derart automatisch aufgebauter Netzwerkzugang kann zur Bereitstellung von ein oder mehreren Diensten, wie z.B. einem Firmware-Update des Geräts 130, durch die Netzwerkeinheit 102 verwendet werden. Dies kann ggf. automatisch ohne Interaktion mit dem Nutzer eingerichtet und/oder angeboten werden, z.B. bei Erstinbetriebnahme des Geräts 130 (ggf. erst nach Zustimmung des Nutzers).

[0038] Insbesondere in einem urbanen Umfeld (z.B. in einem Mehrfamilienhaus) kann es vorteilhaft sein, den Zugang zu der Netzwerkeinheit 102 zumindest in einem ersten Schritt bei Bedarf über ein Hilfs-LAN 111, z.B. über das LAN 111 eines Nachbarn, zu ermöglichen. So kann die verfügbare Netzwerkabdeckung zur Einbindung des Geräts 130 erweitert werden. Dabei kann der Hilfs-Zugangspunkt 110 darauf beschränkt sein, die Verbindung des Geräts 130 mit der Netzwerkeinheit 102 zu ermöglichen.

[0039] In einem weiteren Schritt kann das Gerät 130 über eine Methode, wie dem OAUTH (Open Authorization) Device Grant, mit einem oder mehreren Nutzerkonten des Nutzers (auf der Netzwerkeinheit 102)

verknüpft werden. Dabei kann das Gerät 130 ggf. auch Zugangsinformation zu der Netzwerkinfrastruktur, insbesondere zu dem Zugangspunkt 120, des Nutzers erhalten. Insbesondere kann eine Einbindung des Geräts 130 in das LAN 121 des Nutzers erfolgen. Der zuvor möglicherweise isolierte und/oder beschränkte (W)LAN-Zugang über den Hilfs-Zugangspunkt 110 kann dadurch auf einen unbeschränkten Zugang des Geräts 130 über einen zweiten Zugangspunkt 120 überführt werden. Das Gerät 130 ist dann ein vollwertiges, authentifiziertes Netzwerkgerät in dem (W)LAN 121 des Nutzers.

[0040] Es wird somit ein Verfahren beschrieben, mit dem ein Netzwerk-fähiges Gerät 130 ggf. ohne Interaktion mit einem Nutzer initial in ein (Hilfs-) Netzwerk 111 eingebunden werden kann und automatisiert ein oder mehrere Berechtigungen erhält, auf eine bestimmte Ressource 102, z.B. auf einen bestimmten Rechner im Internet, zuzugreifen. Insbesondere kann es dabei einem Nutzer vermittelt werden, welches Gerät 130 auf welche Ressource 102 Zugriff hat.

[0041] Durch eine Entität, z.B. durch den Hersteller eines Gerätes 130 oder durch die WIFI-Alliance, kann eine Infrastruktur für private Schlüssel bereitgestellt werden, durch die Zertifikate ausgegeben werden. Die ausgegebenen Zertifikate entsprechen dabei bevorzugt einem verbreiteten Standard, z.B. x.509. Zertifikate können dann (geeignet codiert) auf den beteiligten Komponenten, insbesondere auf ein oder mehreren Geräten 130 und auf ein oder mehreren Zugangspunkten 110, 120, abgelegt werden. Private Schlüssel können in sicherer Weise auf sogenannten Trusted-Platform-Modules (TPM) abgelegt werden, und können ggf. auf den jeweiligen TPMs erzeugt werden.

[0042] Innerhalb der PKI (Public Key Intrastructure) existiert ggf. nur ein Stammzertifikat mit einer möglichst langen Lebensdauer, z.B. 30 Jahre. Alle anderen Zertifikate können von dem Stammzertifikat über ein oder mehrere Zwischenzertifikate (ggf. auch mehrstufig) abgeleitet werden. So kann für unterschiedliche Gruppen von Geräten 130 (z.B. für unterschiedliche Hersteller von Geräten 130) jeweils ein Zertifikatsbaum erstellt werden, der für die Geräte 130 der jeweiligen Gruppe eineindeutig ist, und dessen Blätter bestimmten Teilbäumen (z.B. „Fabrik 1“, „Fabrik 2“, ...) zugeordnet sein können. Der Zertifikatsbaum einer Entität (z.B. eines Herstellers) kann dabei ein Stammzertifikat aufweisen, von dem alle Zertifikate der Gruppe von Geräten 130 der Entität abgeleitet werden.

[0043] Die Zertifikate und/oder Zwischenzertifikate können mit geeigneten Metadaten erstellt werden, durch die z.B. Information zur jeweiligen ausstellenden Instanz des jeweiligen Zertifikats bereitgestellt wird.

[0044] Über geeignete Protokolle und/oder Dienste, wie OCSP (Online Certificate Status Protocol)-Responding und/oder OCSP-Stapling, kann jederzeit die Validität eines Zertifikats überprüft werden. Des Weiteren kann der Austausch von Zertifikaten in unterschiedlichen Netzwerkgeräten 130 über geeignete, ggf. standardisierte Methoden, umgesetzt werden.

[0045] Ein Netzwerkgerät 130 kann, z.B. während der Herstellung, mit einer digitalen Identität und mit mindestens einem Zertifikat ausgestattet werden. Das Zertifikat kann dabei von einem der Zwischenzertifikate des entsprechenden Teilbaumes des Zertifikatbaums signiert und im Gerät gemeinsam mit dem privaten Schlüssel sicher innerhalb eines geeigneten Speichers (z.B. einem TPM) abgelegt sein.

[0046] Des Weiteren kann die Zertifikatskette bis zu dem Stammzertifikat oder bis zu einem von dem Stammzertifikat abgeleiteten Referenzzertifikat im Gerät 130 abgelegt sein, und kann z.B. beim Verbindungsaufbau zu einem Zugangspunkt 110, 120 übertragen werden, bzw. kann über einen anderen Mechanismus dem Zugangspunkt 110, 120 bekannt gemacht werden. In dem Zertifikat des Geräts 130 kann auch gespeichert sein, unter welcher Internetadresse das jeweilige Stammzertifikat abrufbar ist.

[0047] Das Stammzertifikat bzw. das von dem Stammzertifikat abgeleitete Referenzzertifikat für eine Gruppe von Geräten 130 kann in ein oder mehreren Zugangspunkten oder Routern 110, 120 bereitgestellt werden. Insbesondere können die an dem System 100 teilnehmenden Hersteller bzw. die WIFI-Alliance auf einem geeignete Wege Kopien ihres jeweiligen Stammzertifikats (oder davon abgeleiteter Referenzzertifikate) in die Zugangspunkte oder Router 110, 120 übertragen. Ähnlich dem Zertifikatsspeicher eines Webbrowsers erhält ein Zugangspunkt 110, 120 damit Informationen über Vertrauensstellungen, die ggf. bereits bei der Herstellung des Zugangspunkts 110, 120 festgelegt werden können.

[0048] **Fig. 2a** zeigt eine beispielhafte Liste 200 mit ein oder mehreren Stamm- oder Referenzzertifikaten 201 für entsprechende ein oder mehrere Entitäten (z.B. Hersteller). Für jede Entität kann dabei ggf. zumindest eine Netzwerkeinheit 102 (z.B. zumindest ein Internet-Server) in der Liste 200 angezeigt werden, auf den über den Zugangspunkt 110, 120 zugegriffen werden kann. Die ein oder mehreren Netzwerkeinheiten 102 können innerhalb der Liste 200 in einem Feld 202 für Zugriffsrechte aufgeführt sein.

[0049] Fig. 2b zeigt eine beispielhafte Zertifikatskette 210 mit ein oder mehreren Zwischenzertifikaten 212 zwischen dem Geräte-Referenzzertifikat 211 einer Entität und dem Zertifikat 213 des Geräts 130. Die Zertifikatskette 210 kann auf dem Gerät 130 gespeichert sein. Alle Zwischenzertifikate 212 und das Geräte-Zertifikat 213 werden sequentiell aus dem Geräte-Referenzzertifikat 211 abgeleitet. Das Geräte-Referenzzertifikat 211 einer Entität (z.B. eines Geräte-Herstellers) kann z.B. das Stammzertifikat der Entität sein. Wie durch die Pfeile in **Fig. 2b** dargestellt, können aus dem Referenzzertifikat 211 und/oder aus einem Zwischenzertifikat 212 unterschiedliche Geräte-Zertifikate 213 für unterschiedlichen Geräte 130 abgeleitet werden.

[0050] Sobald ein Gerät 130 mit Strom versorgt wird, kann es ggf. damit beginnen, über eine geeignete Methode, z.B. das Device-Provisioning-Protocol (DPP), nach einem geeigneten Zugangspunkt 110 zu suchen, in dem das Stamm- bzw. Referenzzertifikat 201, 211 zu dem Zertifikat 213 des Geräts 130 hinterlegt ist. Die genaue Vorgehensweise wird dabei von dem jeweils verwendeten Protokoll vorgegeben.

[0051] Wenn ein geeigneter Zugangspunkt 110 gefunden wird, kann mit Hilfe des öffentlichen Schlüssels eine sichere LAN-Verbindung 112 zu dem Zugangspunkt 110 hergestellt werden und es kann die jeweilige Zertifikatskette 210 übertragen werden. Die bereitgestellte Zertifikatskette 210 weist dabei eine ausreichende Tiefe auf, um es dem Zugangspunkt 110 zu ermöglichen, die von dem Gerät 130 bereitgestellte Zertifikatskette 210 einem intern vorhandenen Stammzertifikat 201 zuordnen zu können. Wenn die Zertifikatskette 210 erfolgreich zugeordnet werden konnte, dann kann eine Freigabe zumindest einer Ressource 102 für das Gerät 130 erfolgen.

[0052] Sobald eine Verbindung zwischen dem Gerät 130 und dem Zugangspunkt 110 auf Netzwerkebene zustande gekommen ist, kann das ins Netzwerk 111 zu integrierende Gerät 130 mit dynamisch festgelegten Daten höherer Protokollschichten provisioniert werden. Die dafür erforderliche Berechtigung kann z.B. durch ein gemeinsames Geheimnis bereitgestellt werden (was jedoch den vorhergehenden Austausch des Geheimnisses, z.B. eines Passwortes, erfordert).

[0053] Bei Vorliegen eines dem Zugangspunkt 110 bekannten Stamm- bzw. Referenzzertifikats 201, 211 kann automatisch (ohne vorhergehenden Austausch eines Geheimnisses) eine Zugangsberechtigung gewährt werden. So kann in besonders komfortabler und effizienter Weise ein Verbindungsaufbau ermöglicht werden. Insbesondere kann automatisch nach Einschalten des Geräts 130 die Verbindung 112 zu dem Zugangspunkt 110 aufgebaut werden, und der Zugangspunkt 110 erteilt daraufhin automatisch den Zugang zu höheren Protokollen und/oder den Zugang zu ein oder mehreren bestimmten Routing-Zielen 102.

[0054] Insbesondere kann ein Netzwerkgerät 130 eines dem Zugangspunkt 110 bekannten Herstellers automatisch für (zumindest oder genau) eine, z.B. im Stamm- oder Referenzzertifikat 201, 211 explizit angegebene, Netzwerkeinheit 102 im Internet freigeschaltet sein. Für den Zugriff auf die Netzwerkeinheit 102 ist dabei keine Nutzerinteraktion erforderlich. Ein Zugriff auf andere Ressource, z.B. das lokale interne Netzwerk 110 und/oder andere Ziele / Endpunkte im Internet können andererseits unterbunden werden.

[0055] Beispielsweise kann in einer x.509-Erweiterung des Stamm- bzw. Referenzzertifikats 201, 211 festgehalten werden, auf welche ein oder mehreren Internetadressen („Domain-Namen“) die Geräte 130 einer bestimmten Stammzertifizierungsstelle bzw. einer bestimmten Entität Zugriff haben sollen. Der Zugriff kann dann durch den Zugangspunkt 110 auf die explizit angegebenen Internetadressen beschränkt sein. Von einem Gerät 130 ausgehender Datenverkehr an andere Adressen oder über andere Protokolle kann dann automatisiert von dem Zugangspunkt 110 verworfen werden.

[0056] Sofern ein Gerät 130 einen Verbindungsaufbau zu dem Zugangspunkt 110 versucht, das nicht über die an dem Zugangspunkt 110 hinterlegte Liste 200 bekannter Zertifizierungsstellen autorisiert ist, kann der Datenverkehr des Geräts 130 automatisch von dem Zugangspunkt 110 blockiert werden. Alternativ oder ergänzend kann dem Nutzer eine Auswahl angeboten werden, ob das betroffene Gerät 130 manuell autorisiert werden soll.

[0057] Sofern mehrere Zugangspunkte 110, 120 mit entsprechender Berechtigung in Reichweite des Geräts 130 liegen, kann das Gerät 130 nach einem geeigneten Verfahren (z.B. in Abhängigkeit von der jeweils höchsten Signalstärke und/oder der jeweils größten Datenrate) eine Auswahl für den bevorzugten Zugangspunkt 110, 120 treffen. Dabei kann es ggf. auch ermöglicht werden, einen Zugangspunkt 110, 120 auszuwählen, der nicht durch den Nutzer (sondern z.B. durch einen Nachbarn) betrieben wird.

[0058] Im Anschluss an eine (beschränkte) Einbindung in ein erstes LAN 111 kann eine nachträgliche Einbindung in ein weiteres zweites LAN 121 erfolgen (z.B. um eine unbeschränkte Einbindung und/oder einen unbeschränkten Zugriff zu ermöglichen). Das zweite LAN 121 kann dabei das von dem Nutzer betriebene LAN sein. Zu diesem Zweck kann WPS (Wi-Fi Protected Setup) genutzt werden, es kann das WIFI-Passwort eingegeben werden und/oder es

kann ggf. auch eine beliebige andere Methode wie Captive-Portal- und Soft-Access-Point verwendet werden.

[0059] In einem bevorzugten Beispiel kann dem Nutzer auf der Netzwerkeinheit 102 ein Nutzerkonto bereitgestellt werden, auf dem z.B. der Zugangspunkt 120 des Nutzers registriert ist. In dem Nutzerkonto kann eine Zugangspunktzuordnung inklusive der Zugangsdaten der ein oder mehreren Netzwerkgeräte 130 des Nutzers zu einem bestimmten Zugangspunkt 120 verwaltet werden. Dabei kann es ermöglicht werden, ein Gerät 130, das zunächst über einen fremden Zugangspunkt 110 mit der Netzwerkeinheit 102 verbunden wird, in das Nutzerkonto einzubinden. Hierzu kann z.B. die Methode OAUTH Device Grant verwendet werden.

[0060] Sobald die Verknüpfung des Geräts 130 zu dem Nutzerkonto hergestellt wurde, kann die Netzwerkeinheit 102 einen geeigneten Zugangspunkt 120 für das Gerät 130 auswählen (z.B. in Abhängigkeit von der durch das Netzwerkgerät 130 beobachteten Signalstärke der möglichen Zugangspunkte 120). Die für den Zugang zu dem auswählten Zugangspunkt 120 erforderlichen Zugangsdaten können dann an das Netzwerkgerät 130 übertragen werden. Das Gerät 130 kann sich dann automatisch mit dem Zugangspunkt 120 verbinden.

[0061] Alternativ oder ergänzend zu einer automatischen Bereitstellung eines Stamm- bzw. Referenzzertifikats 201, 211 und eines damit verknüpften Zugriffsrechts auf eine Netzwerkeinheit 102 kann es einem Nutzer ermöglicht werden, einen Zugangspunkt 110, 120 manuell zu konfigurieren (über eine Benutzerschnittstelle). Beispielsweise kann es einem Nutzer ermöglicht werden, über ein Anwendergerät 140 (z.B. ein Smartphone oder ein Computer) auf einen Zugangspunkt 110, 120 zuzugreifen (etwa über eine LAN-Verbindung 124), um die Liste 200 mit ein oder mehreren Stamm- bzw. Referenzzertifikaten 201, 211 und/oder mit Einträgen 202 für die Zugriffsrechte auf ein oder mehrere Netzwerkeinheiten 102 zu editieren.

[0062] Ein Zugangspunkt 110, 120 kann dem Nutzer z.B. eine Übersicht zur Verfügung stellen (z.B. über die Benutzerschnittstelle), z.B. mit folgender Information und/oder mit folgenden Möglichkeiten:

- die ein oder mehreren installierte Stamm- bzw. Referenzzertifikate 201 können angezeigt werden;
- ein oder mehrere Parameter für jedes Stamm- bzw. Referenzzertifikat 201 bzw. nötige Berechtigungen hierfür können angezeigt werden, z.B.: Endpunkt(e) 102 im Internet, Datenrate, Dienste, Protokolle, benötigte Ressourcen, etc.;
- eine Möglichkeit, pro Netzwerkgerät 130 ein oder mehrere Beschränkungen zu editieren, aufzuerlegen oder aufzuheben:
  - ○ Zugriff auf bestimmte Endpunkte 102, z.B. die Infrastruktur des Herstellers;
  - ○ Protokolle (IP*, http*, ...);
  - ○ Dienste (z.B. einen Zeitserver);
  - ○ 2eitere Parameter (Datenrate, Zeitbeschränkungen des Zugriffs, ...);
- ein Status pro Netzwerkgerät 130 kann angezeigt werden, z.B. Verbindung aktiv, aktuelle Datenrate, akkumuliertes Datenvolumen, genutzte Dienste („Hersteller-Backend“, „Zeitserver“, ...), Fehlerzustände („Stamm- bzw. Referenzzertifikat abgelaufen“, ...); und/oder
- eine allgemeine Einstellung kann vorgenommen werden, wie etwa eine Benachrichtigungseinstellung, wenn sich ein neues Gerät 130 über das beschriebene Verfahren verbunden hat oder einen Verbindungsaufbau wünscht.

[0063] Diese Information kann ggf. im lokalen Netzwerk 111, 121 über Methoden und Protokolle, z.B. uPNP oder HTTP, abrufbar sein, und kann ggf. von geeigneten Agenten, Mobilgeräten 140, Webbrowsern oder ähnlich, ausgewertet und verändert werden.

[0064] Durch die in diesem Dokument beschriebenen Maßnahmen kann es einem Nutzer eines Geräts 130 ermöglicht werden, das Gerät 130 in besonders komfortabler und sicherer Weise in ein LAN 111, 121 einzubinden, und ggf. mit einer Netzwerkeinheit 102 in einem WAN zu verbinden (z.B. für Wartungstätigkeiten, für ein Firmware-Update, etc.).

[0065] **Fig. 3a** zeigt ein Ablaufdiagramm eines beispielhaften Verfahrens 300 zur Einbindung eines Geräts 130, insbesondere eines Hausgeräts, etwa einer Küchenmaschine, eines Ofens, einer Waschmaschine, eines Herds, eines Kühlschranks, einer Spülmaschine, eines Trockners, etc., in ein Local Area Network (LAN) 111, und ggf. darüber in ein WAN. Das Verfahren 300 kann durch einen Zugangspunkt 110 (insbesondere durch einen Router) zu einem LAN 111 ausgeführt werden. Der Zugangspunkt 110 kann dabei ausgebildet sein, ein Wireless LAN (WLAN) bereitzustellen.

[0066] Das Gerät 130 kann ein Zertifikat 213 aufweisen, das aus einem Geräte-Referenzzertifikat 211 abgeleitet wurde. Dabei kann das Zertifikat 213 des Geräts 130 über eine Zertifikatskette 210 (mit ein oder mehreren Zwischenzertifikaten 212) aus dem Geräte-Referenzzertifikat 211 generiert worden sein. Das Gerät 130 kann ausgebildet sein, die Zertifikatskette 210 bereitzustellen. Das Zertifikat 213 des

Geräts sowie die eventuell vorgehaltene Zertifikatskette 210 können auf einem Trusted-Platform-Module (TPM) des Geräts 130 gespeichert sein.

[0067] Das Verfahren 300 umfasst das Überprüfen 301, ob das Zertifikat 213 des Geräts 130 zu zumindest einem Referenzzertifikat 201 passt, das an einem ersten Zugangspunkt 110 zu einem ersten LAN 111 verfügbar ist. Insbesondere kann überprüft werden, ob an dem ersten Zugangspunkt 110 das Geräte-Referenzzertifikat 211 der Entität (d.h. das Referenzzertifikat 201, 211 aus dem das Zertifikat 213 des Geräts 130 abgeleitet wurde) verfügbar ist. Auf einer Speichereinheit, insbesondere auf einem TPM, des ersten Zugangspunktes 110 kann eine Liste 200 mit ein oder mehreren Referenzzertifikaten 201 (z.B. für entsprechende ein oder mehrere Hersteller von Geräten 130) gespeichert sein. Für jedes Referenzzertifikat 201 kann zumindest eine Netzwerkeinheit 102 angegeben sein (als Listeneintrag 202), für die ein Zugriff über den ersten Zugangspunkt 110 ermöglicht wird, wenn das Gerät 130 ein zu dem jeweiligen Referenzzertifikat 201 passendes Zertifikat 213 aufweist. Es können somit Zugangspunkte 110 (insbesondere Router) bereitgestellt werden, die für ausgewählte Geräte 130 einen automatischen (begrenzten) LAN- und ggf. Internet-Zugriff ermöglichen.

[0068] Das Verfahren 300 umfasst ferner das Einbinden 302 des Geräts 130 in das erste LAN 111, wenn (ggf. nur dann, wenn) ermittelt wird, dass das Zertifikat 213 des Geräts 130 zu zumindest einem an dem ersten Zugangspunkt 110 verfügbaren Referenzzertifikat 201 passt. Das Einbinden 302 kann dabei automatisch erfolgen, ohne dass der Nutzer des Geräts 130 eine Eingabe tätigen muss. Somit kann ein komfortabler und sicherer Zugriff zu einem LAN 111 und/oder zu einer Netzwerkeinheit 102 in einem WAN ermöglicht werden.

[0069] **Fig. 3b** zeigt ein Ablaufdiagramm eines beispielhaften Verfahrens 310 zur Einbindung eines Geräts 130 in ein LAN 111, 121 und/oder in ein WAN. Das Verfahren 310 kann in komplementärer Weise zu dem Verfahren 300 durch das Gerät 130 ausgeführt werden. Das Gerät 130 weist dabei ein Zertifikat 213 auf, das aus einem Geräte-Referenzzertifikat 211 einer Entität abgeleitet wurde.

[0070] Das Verfahren 310 umfasst das Identifizieren 311 eines ersten Zugangspunkts 110 für ein erstes LAN 111, an dem ein Referenzzertifikat 201 einer Entität verfügbar ist, das zu dem Zertifikat 213 des Geräts 130 passt, insbesondere das dem Geräte--Referenzzertifikat 211 entspricht. Zu diesem Zweck kann das Gerät 130 ggf. mehrere unterschiedliche Zugangspunkte 110, 120 kontaktieren. Es kann dann jeweils das Zertifikat 213 des Geräts 130 (insbesondere die Zertifikatskette 210 des Geräts 130) an den jeweiligen Zugangspunkt 110, 120 gesendet werden. Der jeweilige Zugangspunkt 110, 120 kann dann überprüfen, ob das zu dem Zertifikat 213 passende Referenzzertifikat 201 (insbesondere das Geräte-Referenzzertifikat 211) auf dem jeweiligen Zugangspunkt 110, 120 verfügbar ist. Der Prozess des Identifizierens 311 eines geeigneten Zugangspunkts 110 kann dabei automatisch von dem Gerät 130 initiiert werden (ohne Eingabe des Nutzers), z.B. bei Inbetriebnahme des Geräts 130.

[0071] Das Verfahren 310 umfasst ferner das Einbinden 312 des Geräts 130 in das erste LAN 111 über den (identifizierten) ersten Zugangspunkt 110. So kann ein komfortabler und sicherer Zugang zu einem LAN 111 (insbesondere einem WLAN) ermöglicht werden.

[0072] Die vorliegende Erfindung ist nicht auf die gezeigten Ausführungsbeispiele beschränkt. Insbesondere ist zu beachten, dass die Beschreibung und die Figuren nur das Prinzip der vorgeschlagenen Verfahren und Vorrichtungen veranschaulichen sollen.

Patentansprüche

1. Verfahren (300) zur Einbindung eines Geräts (130) in ein Local Area Network, kurz LAN, (111); wobei das Gerät (130) ein Zertifikat (213) aufweist, das aus einem Geräte-Referenzzertifikat (211) abgeleitet wurde; wobei das Verfahren (300) umfasst,
- Überprüfen (301), ob das Zertifikat (213) des Geräts (130) zu zumindest einem Referenzzertifikat (201) passt, das an einem ersten Zugangspunkt (110) zu einem ersten LAN (111) verfügbar ist;
- Einbinden (302) des Geräts (130) in das erste LAN (111), wenn ermittelt wird, dass das Zertifikat (213) des Geräts (130) zu zumindest einem an dem ersten Zugangspunkt (110) verfügbaren Referenzzertifikat (201) passt;
- Ermitteln von einer Netzwerkeinheit (102), für die eine Zugriffsberechtigung des Geräts (130) über das erste LAN (111) vorliegt; wobei die Netzwerkeinheit (102) zumindest einen zweiten Zugangspunkt (120) zu einem zweiten LAN (121) anzeigt; und
- Aufbauen einer Kommunikationsverbindung zwischen dem Gerät (130) und der Netzwerkeinheit (102) über den ersten Zugangspunkt (110), um es dem Gerät (130) zu ermöglichen, Zugangsdaten zu dem zweiten Zugangspunkt (120) von der Netzwerkeinheit (102) zu beziehen.

2. Verfahren (300) gemäß Anspruch 1, wobei
- an dem ersten Zugangspunkt (110) eine Liste (200) mit ein oder mehreren Referenzzertifikaten (201) verfügbar ist; und
- das Verfahren (300) umfasst,
- Bestimmen, ob das Geräte-Referenzzertifikat (211)

in der Liste (200) mit ein oder mehreren Referenzzertifikaten (201) enthalten ist oder nicht; und
- Einbinden (302) des Geräts (130) in das erste LAN (111), wenn, insbesondere nur dann, wenn, bestimmt wird, dass das Geräte-Referenzzertifikat (211) in der Liste (200) mit ein oder mehreren Referenzzertifikaten (201) enthalten ist.

3. Verfahren (300) gemäß Anspruch 2, wobei die Liste (200) mit ein oder mehreren Referenzzertifikaten (201) auf einer Speichereinheit, insbesondere auf einem Trusted-Platform-Module, des ersten Zugangspunktes (110) gespeichert ist.

4. Verfahren (300) gemäß einem der vorhergehenden Ansprüche, wobei
- das Überprüfen (301) umfasst, Überprüfen, auf Basis des Zertifikats (213) des Geräts (130), ob das Geräte-Referenzzertifikat (211) an dem ersten Zugangspunkt (110) verfügbar ist, insbesondere ob das Geräte-Referenzzertifikat (211) auf einer Speichereinheit des ersten Zugangspunkts (110) gespeichert ist; und
- das Gerät (130) über den ersten Zugangspunkt (110) in das erste LAN (111) eingebunden wird, wenn, insbesondere nur dann, wenn, ermittelt wird, dass das Geräte-Referenzzertifikat (211) an dem ersten Zugangspunkt (110) verfügbar ist.

5. Verfahren (300) gemäß einem der vorhergehenden Ansprüche, wobei das Verfahren (300) umfasst,
- Ermitteln von ein oder mehreren Netzwerkeinheiten (102), für die eine Zugriffsberechtigung des Geräts (130) über das erste LAN (111) vorliegt; und
- Beschränken der Einbindung des Geräts (130) in das erste LAN (111) auf den Zugriff zu den ein oder mehreren Netzwerkeinheiten (102).

6. Verfahren (300) gemäß Anspruch 5, wobei
- die ein oder mehreren Netzwerkeinheiten (102) in einem Wide Area Network, kurz WAN, außerhalb des ersten LAN (111) angeordnet sind; und
- das Verfahren (300) umfasst, Bereitstellen einer Kommunikationsverbindung zwischen dem Gerät (130) und den ein oder mehreren Netzwerkeinheiten (102) über den ersten Zugangspunkt (110), insbesondere über einen Router des ersten Zugangspunktes (110).

7. Verfahren (300) gemäß einem der Ansprüche 5 bis 6, wobei
- an dem ersten Zugangspunkt (110) eine Liste (200) mit ein oder mehreren Referenzzertifikaten (201) verfügbar ist; und
- die Liste (200) für jedes der Referenzzertifikate (201) jeweils zumindest eine Netzwerkeinheit (102) anzeigt, für die Geräte (130), die ein zu dem jeweiligen Referenzzertifikat (201) passendes Zertifikat (213) aufweisen, eine Zugriffsberechtigung aufweisen.

8. Verfahren (300) gemäß einem der vorhergehenden Ansprüche, wobei das Verfahren (300) umfasst,
- Ermitteln einer Geräte-Zertifikatskette (210) zwischen dem Zertifikat (213) des Geräts (130) und dem Geräte-Referenzzertifikat (211); wobei die Geräte-Zertifikatskette (210) ein oder mehrere Zwischenzertifikate (212) zwischen dem Zertifikat (213) des Geräts (130) und dem Geräte-Referenzzertifikat (211) anzeigt; und
- Überprüfen, auf Basis der Geräte-Zertifikatskette (210), ob das Zertifikat (213) des Geräts (130) zu zumindest einem Referenzzertifikat (201) passt, das an einem ersten Zugangspunkt (110) zu dem ersten LAN (111) verfügbar ist.

9. Verfahren (310) zur Einbindung eines Geräts (130) in ein Local Area Network, kurz LAN, (111, 121); wobei das Gerät (130) ein Zertifikat (213) aufweist, das aus einem Geräte-Referenzzertifikat (211) abgeleitet wurde; wobei das Verfahren (310) umfasst,
- Identifizieren (311) eines ersten Zugangspunkts (110) für ein erstes LAN (111), an dem ein Referenzzertifikat (201) verfügbar ist, das zu dem Zertifikat (213) des Geräts (130) passt, insbesondere das dem Geräte-Referenzzertifikat (211) entspricht;
- Einbinden (312) des Geräts (130) in das erste LAN (111) über den ersten Zugangspunkt (110);
- Zugreifen auf eine Netzwerkeinheit (102) über den ersten Zugangspunkt (110); wobei die Netzwerkeinheit (102) zumindest einen zweiten Zugangspunkt (120) zu einem zweiten LAN (121) anzeigt; und
- Beziehen von Zugangsdaten zu dem zweiten Zugangspunkt (120) von der Netzwerkeinheit (102).

10. Verfahren (310) gemäß Anspruch 9, wobei das Verfahren (310) umfasst,
- Einbinden des Geräts (130) in das zweite LAN (121) über den zweiten Zugangspunkt (120) unter Verwendung der Zugangsdaten zu dem zweiten Zugangspunkt (120); und/oder
- Abmelden des Geräts (130) von dem ersten Zugangspunkt (110).

11. Verfahren (310) gemäß einem der Ansprüche 9 bis 10, wobei das Verfahren (310) umfasst,
- Aufbauen einer Kommunikationsverbindung zu einer Netzwerkeinheit (102) über den ersten Zugangspunkt (110); und
- Bewirken einer Wartungsmaßnahme des Geräts (130) durch Zugriff der Netzwerkeinheit (102) auf das Gerät (130) über den ersten Zugangspunkt (110).

12. System mit einem Gerät (130) und einem ersten Zugangspunkt (110) zu einem ersten Local

Area Network, kurz LAN, (111); wobei das Gerät ein Zertifikat (213) aufweist, das aus einem Geräte-Referenzzertifikat (211) abgeleitet wurde und das Gerät (130) dazu eingerichtet ist,
- den ersten Zugangspunkt (110) für das erste LAN (111) zu identifizieren, an dem ein Referenzzertifikat (201) verfügbar ist, das zu dem Zertifikat (213) des Geräts (130) passt; und
- in Reaktion darauf, eine Einbindung in das erste LAN (111) über den ersten Zugangspunkt (110) zu bewirken wobei der erste Zugangspunkt (110) eingerichtet ist,
- zu überprüfen, ob das Zertifikat (213) des Geräts (130), das in das erste LAN (111) eingebunden werden soll, zu dem Referenzzertifikat (201) passt, das an dem ersten Zugangspunkt (110) verfügbar ist; und
- das Gerät (130) in das erste LAN (111) einzubinden, wenn ermittelt wird, dass das Zertifikat (213) des Geräts (130) zu dem an dem ersten Zugangspunkt (110) verfügbaren Referenzzertifikat (201) passt;
- wobei das System dazu eingerichtet ist,
- eine Netzwerkeinheit (102) zu ermitteln, für die eine Zugriffsberechtigung des Geräts (130) über das erste LAN (111) vorliegt; wobei die Netzwerkeinheit (102) zumindest einen zweiten Zugangspunkt (120) zu einem zweiten LAN (121) anzeigt; und
- über den ersten Zugangspunkt (110) eine Kommunikationsverbindung zwischen dem Gerät (130) und der Netzwerkeinheit (102) aufzubauen, um es dem Gerät (130) zu ermöglichen, Zugangsdaten zu dem zweiten Zugangspunkt (120) von der Netzwerkeinheit (102) zu beziehen.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

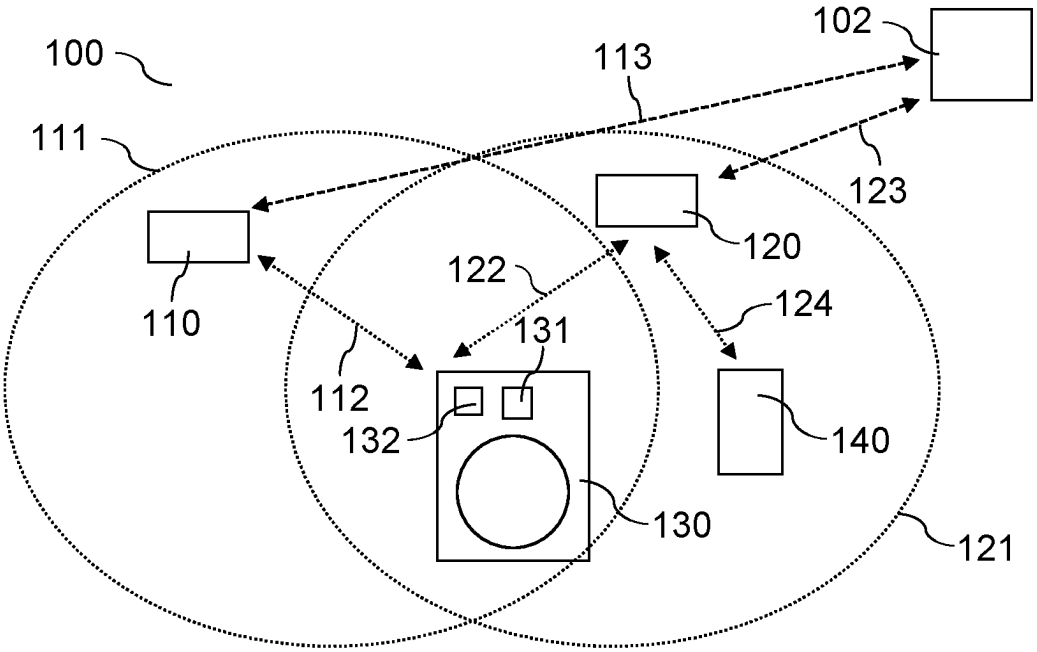


Fig. 1

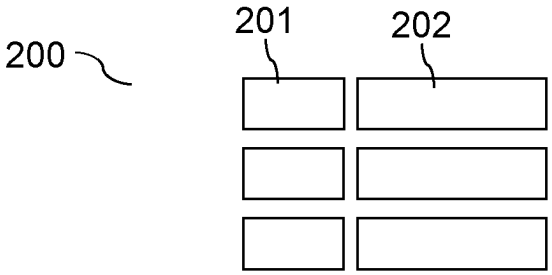


Fig. 2a

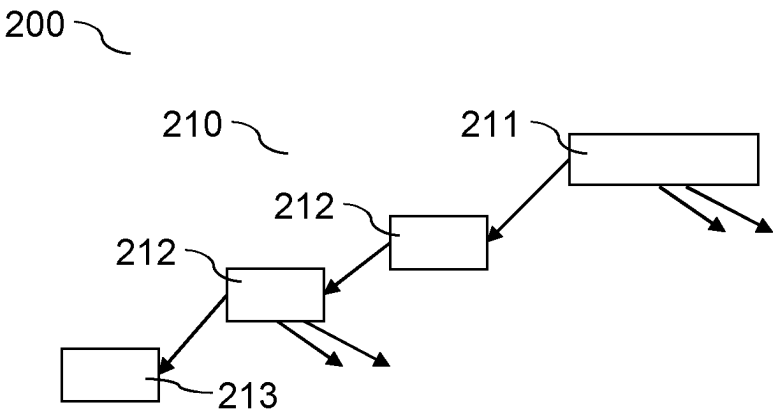


Fig. 2b

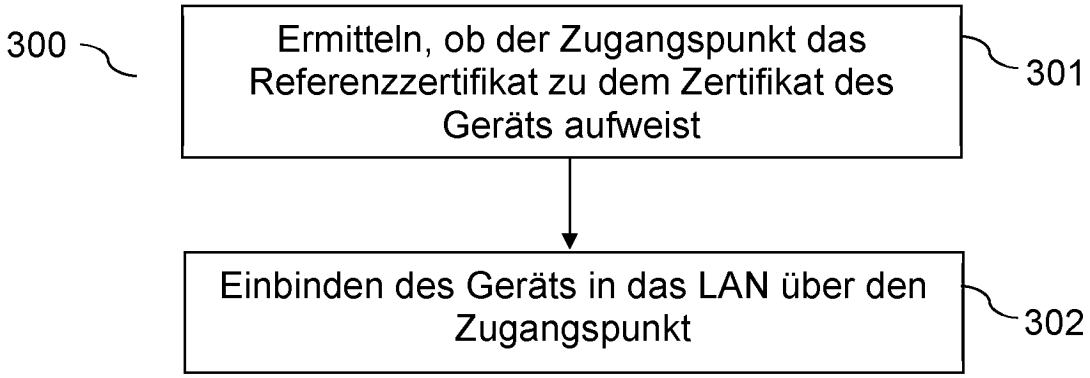


Fig. 3a

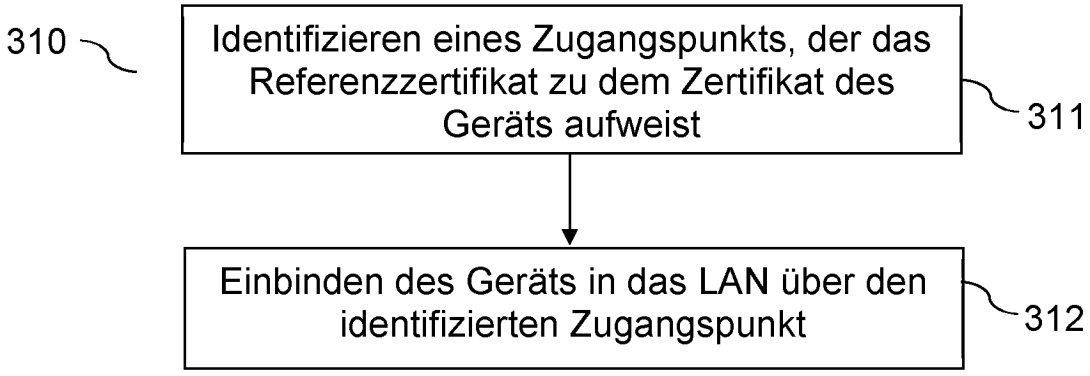


Fig. 3b

