
Verfahren zur Kommunikation von IoT Knoten oder IoT Geräten in einem lokalen Netzwerk

Die vorliegende Erfindung betrifft ein Verfahren zur Kommunikation von IoT Knoten oder IoT Geräten in einem lokalen Netzwerk sowie ein lokales Netzwerk mit einer Mehrzahl von IoT Knoten oder IoT Geräten.

Zur Verbesserung der Automatisierung werden immer mehr Sensoren und Aktoren eingesetzt, welche netzwerkfähig sind. Derartige Netzwerke werden als Internet der Dinge oder Internet of Things IoT oder als industrielles Internet der Dinge Industrial Internet of Things IIoT bezeichnet. Eine Kommunikation zwischen den Sensoren und den Aktoren basiert typischerweise auf einem IP Protokoll. Hierbei können diese Sensoren und Aktoren in einem lokalen Netzwerk (Smart Home oder in einer Fabrik) eingesetzt werden. Alternativ dazu können diese IoT Sensoren und Aktoren auch unmittelbar mit dem Internet verbunden sein.

Insbesondere bei der Verwendung von IoT Sensoren in einem lokalen Netzwerk muss die Sicherheit der internen Kommunikation gewährleistet sein.

In der prioritätsbegründenden deutschen Patentanmeldung hat das Deutsche Patent- und Markenamt die folgenden Dokumente recherchiert: US 2020/0259667 A1 und WO 2020/143982 A1.

Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren zur Kommunikation von IoT Knoten oder IoT Geräten in einem lokalen Netzwerk mit einer verbesserten Sicherheit zu ermöglichen.

Diese Aufgabe wird durch ein Verfahren zur Kommunikation von IoT Knoten oder IoT Geräten in einem lokalen Netzwerk gemäß Anspruch 1 und durch ein Lokales Internet-of-Things IoT Netzwerk nach Anspruch 7 gelöst.

Somit wird ein Verfahren zur Kommunikation von IoT Knoten oder IoT Geräten in einem lokalen Netzwerk vorgesehen, das nur über einen Computer zumindest teilweise mit dem Internet verbunden ist. Das lokale Netzwerk (z.B. ein Local Area Network LAN) stellt ein Ethernet Netzwerk oder ein Single Pair Ethernet Netzwerk dar. Die IoT Knoten oder die IoT

5 Geräte sind displaylos und bedienungselementefrei ausgestaltet. Ferner weisen sie eine erste Schnittstelle zur Kommunikation in dem lokalen Netzwerk mit anderen IoT Knoten oder dem Computer auf. Jeder IoT Knoten oder jedes IoT Gerät weist einen ersten öffentlichen kryptographischen Schlüssel und einen ersten privaten kryptographischen Schlüssel auf. Der erste private Schlüssel ist vorab in dem IoT Knoten oder dem IoT Gerät abgelegt

10 oder wird von diesem erzeugt. Eine Authentifizierung der IoT Knoten oder der IoT Geräte in dem lokalen Netzwerk erfolgt durch Senden einer Anfrage nach einem Root-Zertifikat durch den Computer an einen Root-Zertifikat Server im Internet, der mindestens ein Root-Zertifikat eines Herstellers der IoT Knoten oder der IoT Geräte aufweist. Das Root-Zertifikat wird durch den Computer empfangen und gespeichert. Der Computer überprüft, ob die in

15 dem lokalen Netzwerk vorhandenen IoT Knoten oder IoT Geräte originale und unveränderte Geräte darstellen. Dies erfolgt anhand des empfangenen Root-Zertifikats. Das Root-Zertifikat ist dazu geeignet, den ersten öffentlichen Schlüssel der IoT Knoten oder der IoT Geräte mit einer eindeutigen Adressinformation des IoT Knotens oder des IoT Gerätes zu verknüpfen. Die eindeutigen Adressinformationen können Adressinformationen darstellen,

20 die ausschließlich in dem lokalen Netzwerk gültig ist. Der Computer überprüft anhand des gespeicherten Root-Zertifikats, ob der öffentliche Schlüssel des IoT Knotens oder des IoT Gerätes durch den Hersteller signiert ist. Der erste private kryptographische Schlüssel des IoT Knotens oder des IoT Gerätes wird basierend auf einem kryptographischen Verfahren überprüft.

25 Eine ausschließlich in dem lokalen Netzwerk gültige Adressinformationen unterscheidet sich von der sonst üblichen Vorgehensweise, da typischerweise die Identifikation basierend auf globalen (routing-fähigen) Adressen erfolgt. Diese Adressen sind jedoch vom Einsatzort abhängig und können somit dem Hersteller des Knotens nicht bekannt sein. Daher kann eine Attestation nur indirekt mit Hilfe des Herstellers der IoT Knoten oder Geräte ermöglicht werden. Zudem erhöht sich der Aufwand für Authentifizierungen, da die Routing-

30 fähigen Netzwerknamen einer Verwaltung des Administrators unterliegen und nicht einem ZeroConf-Ansatz (zero configuration) folgen, der ausschließlich lokal gültigen Adressinformationen verwendet. Ein Zero Configuration Netzwerk stellt ein Netzwerk dar, das eine selbstständige Konfiguration ohne Eingriffe eines menschlichen Bedieners erlaubt. Durch

35 die Verwendung von lediglich im lokalen Netzwerk gültige Adressinformationen kann eine

automatische und selbstständige Konfiguration der IoT Sensoren oder Geräte in dem lokalen Netzwerk erfolgen. Die eindeutige lokale Adressinformation kann beispielsweise eine Link Local Address IPv6 oder einen Multicast Domain Name Service Netzwerknamen darstellen.

- 5 Gemäß einem Aspekt der vorliegenden Erfindung kann der Computer nach Empfangen und Speichern des Root-Zertifikats vom Internet getrennt werden, so dass keine aktive Internetverbindung vorhanden ist. Damit kann die weitere Authentifizierung der in dem lokalen Netzwerk vorhandenen IoT Knoten oder der IoT Geräte ohne aktive Internetverbindung und damit anonym erfolgen. Ein Zugriff auf das lokale Netzwerk über das Internet
10 und ein möglicher Angriff auf das lokale Netzwerk kann damit verhindert werden.

- Gemäß einem Aspekt der Erfindung weist der IoT Knoten oder das IoT Gerät lediglich eine erste Schnittstelle zur Kommunikation mit dem Netzwerk und optional eine zweite Schnittstelle zur Kommunikation mit Sensoren oder Aktoren auf, die mit dem IoT gekoppelt sind. Somit ist weder ein Display noch ein Bedienelement oder Eingabeelement vorhanden. Ein-
15 stellungen und Parameter können z.B. über einen Browser auf dem Computer 130 geändert oder angepasst werden.

- Die Erfindung betrifft ebenfalls ein lokales Internet-of-Things IoT Netzwerk. Das Netzwerk weist eine Mehrzahl von Internet-of-Things IoT Knoten oder Geräten auf, welche Displaylos und Bedienungselemente-frei ausgestaltet sind und jeweils eine erste Schnittstelle zur
20 Kommunikation mit dem lokalen Netzwerk mit anderen IoT Knoten oder einem Computer aufweisen. Das Netzwerk weist einen Computer auf, der zumindest teilweise mit dem Internet verbunden ist. Jeder IoT Knoten oder jedes IoT Gerät weist einen ersten öffentlichen kryptographischen Schlüssel und einen ersten privaten kryptographischen Schlüssel auf. Der erste private Schlüssel ist vorab abgelegt oder wird von dem IoT Knoten oder IoT Gerät
25 selber erzeugt. Der Computer ist dazu ausgestaltet, IoT Knoten oder IoT Geräte in dem lokalen Netzwerk zu authentifizieren, indem eine Anfrage nach einem Root-Zertifikat von dem Computer an einen Root-Zertifikat-Server im Internet gesendet wird, der mindestens ein Root-Zertifikat eines Herstellers der IoT Knoten oder der IoT Geräte aufweist. Das Root-Zertifikat wird durch den Computer empfangen und gespeichert und es wird durch den
30 Computer anhand des empfangenen Root-Zertifikats überprüft, ob die IoT Knoten oder IoT Geräte originale und unveränderte Geräte sind. Das Root-Zertifikat ist dazu geeignet, den ersten öffentlichen Schlüssel der IoT Knoten oder IoT Geräte mit einer eindeutigen ausschließlich lokal gültigen Adressinformation des IoT Knotens oder des IoT Gerätes zu verknüpfen. Der Computer ist dazu ausgestaltet, anhand des gespeicherten Root-Zertifikats

zu überprüfen, ob der erste öffentliche Schlüssel der IoT Knoten oder der IoT Geräte durch den Hersteller des IoT Knotens oder des IoT Gerätes signiert sind. Der erste private Schlüssel des IoT Knotens oder des IoT Gerätes wird basierend auf einem kryptographischen Verfahren überprüft.

- 5 Weitere Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Vorteile und Ausführungsbeispiele der Erfindung werden nachstehend unter Bezugnahme auf die Zeichnung näher erläutert.

- | | | |
|----|--------|---|
| | Fig. 1 | zeigt eine schematische Darstellung eines lokalen Netzwerkes gemäß einem ersten Ausführungsbeispiel der Erfindung, |
| 10 | Fig. 2 | zeigt eine vergrößerte Ansicht eines Teils des lokalen Netzwerkes von Fig. 1, |
| | Fig. 3 | zeigt eine schematische Darstellung des lokalen Netzwerkes von Fig. 1 während der Überprüfung der in dem lokalen Netzwerk vorhandenen IoT Knoten, |
| 15 | Fig. 4 | zeigt eine schematische Darstellung eines lokalen Netzwerkes gemäß einem zweiten Ausführungsbeispiel, und |
| | Fig. 5 | zeigt eine schematische Darstellung einer Rücksetzeinheit gemäß einem Ausführungsbeispiel der Erfindung. |

- Fig. 1 zeigt eine schematische Darstellung eines lokalen Netzwerkes gemäß einem ersten
20 Ausführungsbeispiel der Erfindung und Fig. 2 zeigt eine vergrößerte Ansicht eines Teils
des lokalen Netzwerkes von Fig. 1. Ein lokales Netzwerk 100 weist eine Mehrzahl von IoT
(Internet of Things) Knoten 110 auf, welche durch ein Ethernet-Netzwerk oder ein Single
Pair Ethernet-Netzwerk 120 miteinander verbunden sind. Ferner ist ein Computer 130 mit
dem lokalen Netzwerk 120 verbunden. Der Computer 130 kann eine Verbindung mit dem
25 Internet 200 aufbauen. Diese Verbindung mit dem Internet kann wie in Fig. 2 dargestellt
dazu verwendet werden, ein Root-Zertifikat Z für die IoT Knoten 110 in dem lokalen Netz-
werk 100 beispielsweise von einem Root-Zertifikat-Server 210 eines Herstellers der IoT
Knoten 110 abzurufen. Gemäß dem ersten Ausführungsbeispiel hat somit lediglich der
mindestens eine Computer 130 die Möglichkeit, mit dem Internet 200 und insbesondere
30 mit dem Root-Zertifikat-Server 210 zu kommunizieren. Die IoT Knoten 110 können lediglich
innerhalb des lokalen Netzwerkes 120 mit anderen IoT Knoten 110 oder mit dem Computer

130 kommunizieren. Damit sollen die Möglichkeiten eines externen unerlaubten Zugriffs auf die IoT Knoten verringert werden.

Gemäß dem ersten Ausführungsbeispiel weist der mindestens eine Computer 130, welcher mit dem Internet verbindbar ist, ausreichende Mechanismen zum Schutz vor unautorisierten Zugriffen (beispielsweise Firewalls, Antiviren-Software etc.) auf.

Das erste Ausführungsbeispiel der Erfindung betrifft somit insbesondere das Vorsehen der internen Sicherheit des lokalen Netzwerks 100. Insbesondere soll sichergestellt werden, dass die IoT Knoten innerhalb des Netzwerkes 120 originale und unveränderte Geräte darstellen. Damit soll vermieden werden, dass Angriffe oder unerlaubte Zugriffe aus dem Inneren des lokalen Netzwerkes 100 möglich sind. Insbesondere soll vermieden werden, dass IoT Knoten auf andere IoT Knoten zugreifen und Daten auslesen und verändern, ohne dass dies für die Erfüllung ihrer vorgesehenen Aufgabe notwendig wäre.

Gemäß dem ersten Ausführungsbeispiel soll eine automatische Authentifizierung (im Sinne eines Zero Configuration Netzwerkes) der vorhandenen bzw. neu hinzugekommenen IoT Knoten erfolgen. Dies ist insbesondere vorteilhaft, weil damit keine zentralisierten, auf Zertifikaten basierten Sicherheitsmechanismen verwendet werden müssen. Ferner kann auch vermieden werden, dass für jeden IoT Knoten eine Kombination aus Benutzername und Passwort händisch eingegeben werden muss.

Somit kann auch eine automatisierte Maschine-zu-Maschine Kommunikation auch in lokalen Netzwerken mit einer sehr hohen Anzahl von IoT Knoten 110 ermöglicht werden.

Gemäß dem ersten Ausführungsbeispiel soll eine automatische Möglichkeit der Authentifizierung der IoT Knoten 110 innerhalb des lokalen Netzwerkes 100 ermöglicht werden, ohne dass hierbei eine kontinuierliche aktive Internetverbindung beispielsweise zu einem Root-Zertifikat-Server 210 vorhanden sein muss. Dies wird erreicht, indem alle Sicherheitsmechanismen in das lokale Netz verlegt werden, ohne dass bei der Authentifizierung eine aktive Internetverbindung vorhanden sein muss. Hierzu baut der mindestens eine Computer 130 eine aktive Internetverbindung zu einem Root-Zertifikat-Server 210 auf und schickt eine Anforderung nach einem Root-Zertifikat des Herstellers der IoT Knoten 110. Das Root-Zertifikat Z kann auf dem Computer 130 gespeichert werden. Hierbei kann das Zertifikat Z in einem Browser auf dem Computer 130 installiert werden. Danach kann die aktive Internetverbindung getrennt werden, so dass das lokale Netz 110 bzw. der Computer 130 vom Internet 200 getrennt ist.

Die IoT Knoten oder IoT Geräte stellen Geräte dar, die Display-los und Bedienungselemente-frei ausgestaltet sind. Damit können die Kosten für die IoT Knoten oder IoT Geräte reduziert werden. Eine Ansteuerung der IoT Knoten oder IoT Geräte kann nur über das lokale Netzwerk erfolgen. Beispielsweise kann eine Einstellung von Parametern über einen

5 Browser auf dem Computer 130 erfolgen.

Fig. 3 zeigt eine schematische Darstellung des lokalen Netzwerkes von Fig. 1 während der Überprüfung der in dem lokalen Netzwerk vorhandenen IoT Knoten 110. Nachdem die aktive Internetverbindung des Computers 130 mit dem Internet 200 getrennt worden ist, kann der Computer 130 die IoT Knoten 110 in dem lokalen Netzwerk 100 überprüfen. Hierbei

10 kann der Computer 130 zunächst eine Echtheit E überprüfen, d. h. es wird überprüft, ob die vorhandenen IoT Knoten 110 originale und unveränderte IoT Knoten 110 oder IoT Geräte darstellen.

Jedem der IoT Knoten 110 ist ein erster öffentlicher kryptographischer Schlüssel und ein erster privater kryptographischer Schlüssel zugeordnet. Der erste private kryptographische

15 Schlüssel der IoT Knoten 110 kann während der Herstellung des Gerätes durch den Hersteller in dem IoT Knoten 110 gespeichert oder abgelegt werden. Dieser erste private Schlüssel kann derart abgelegt werden, dass er nicht mehr verändert werden kann. Alternativ dazu kann der IoT Knoten 110 dazu ausgestaltet sein, diesen ersten privaten kryptographischen Schlüssel selber zu erzeugen. Jeder IoT Knoten 110 wird ebenfalls bei der

20 Herstellung durch den Hersteller mit einer eindeutigen Adressinformation vorgesehen. Diese eindeutige Adressinformation kann ein ausschließlich im lokalen Netz gültiger Geräte-Name sein. Die eindeutige lokale Adressinformation kann beispielsweise eine Link Local Address IPv6 oder einen Multicast Domain Name Service Netzwerknamen darstellen.

Zur Überprüfung der IoT Knoten 110 kann der Browser des Computers 130 das installierte

25 Root-Zertifikat Z verwenden, um zu überprüfen, ob der öffentliche Schlüssel der IoT Knoten 110 durch den Hersteller der IoT Knoten 110 signiert wurde. Beispielsweise ein Transport Layer Security TLS Verfahren kann dazu verwendet werden, dass anhand des ersten privaten Schlüssels nachgewiesen werden kann, dass der IoT Knoten 110 ein Originalgerät darstellt. Der Vorteil der oben beschriebenen Authentifizierung der IoT Knoten 110 ist, dass

30 dies ohne aktive Internetverbindung erfolgen kann und somit anonym und offline erfolgen kann.

Damit ist eine Device Attestation, d. h. eine Überprüfung der IoT Knoten 110, gewährleistet.

Fig. 4 zeigt eine schematische Darstellung eines lokalen Netzwerkes gemäß einem zweiten Ausführungsbeispiel. Das lokale Netzwerk 100 gemäß dem zweiten Ausführungsbeispiel kann auf dem lokalen Netzwerk 100 gemäß dem ersten Ausführungsbeispiel von Fig. 1 basieren. Somit ist eine Mehrzahl von IoT Knoten 110 über ein Netz 120 miteinander
5 sowie mit einem Computer 130 gekoppelt. In dem zweiten Ausführungsbeispiel sollen diejenigen IoT Knoten 110, welche funktionell zusammen gehören, zu virtuellen lokalen Netzwerken 101, 102 zusammengefügt werden. Dies erfolgt durch eine lokale Public-Key-Infrastruktur PKI. Das erste virtuelle lokale Netzwerk 101 kann somit eine erste lokale Public-Key-Infrastruktur PKI 1 darstellen. Das zweite virtuelle lokale Netzwerk 102 kann eine
10 zweite Public-Key-Infrastruktur PKI 2 darstellen. Derartige virtuelle lokale Netzwerke können in Abhängigkeit der benötigten Anwendung zusammengestellt werden. Gemäß dem zweiten Ausführungsbeispiel kann hierzu ein zweites kryptographisches Schlüsselpaar in dem IoT Knoten 110 erzeugt oder auf den IoT Knoten 110 geladen werden. Das Schlüsselpaar kann durch ein Zertifikat für eine lokale Root Public Key Infrastruktur PKI Instanz
15 signiert sein. Falls ein IoT Knoten 110 in der gewünschten Anwendung als ein Server fungiert, dann kann das PKI Zertifikat als Host-Zertifikat verwendet werden. Anhand dieses Host-Zertifikats können andere IoT Knoten 110 in dem Netzwerk die Identität des Knotens überprüfen und können bei Bedarf eine verschlüsselte Kommunikation aufbauen.

In einem weiteren Beispiel basierend auf dem zweiten Ausführungsbeispiel kann der IoT
20 Knoten 110 sowohl als Server als auch als Client fungieren. Hierbei kann der IoT Knoten 110 beispielsweise als Message Queuing Telemetry Transport MQTT Subscriber/Publisher(Client) oder Broker(Server) oder http-Server fungieren. Hierbei kann für den IoT Knoten 110 ein User Zertifikat auf Basis des kryptographischen Schlüsselpaars erzeugt werden, welches der lokale PKI Root signiert und das auf dem IoT Knoten 110 gespeichert
25 werden kann. Das Zertifikat eines derartigen PKI Roots kann dann optional als vertrauenswürdigen Root Zertifikat auf dem anderen IoT Knoten 110 gespeichert werden. Damit ist ein automatischer Verbindungsaufbau zwischen den IoT Knoten 110 in dem lokalen Netzwerk 100 möglich. Hierbei ist es vorteilhafterweise möglich, dass die IoT Knoten 110, welche die Verbindung aufbauen, sich gegenseitig authentifizieren können und eine verschlüsselte Kommunikation aufbauen können. Insbesondere kann damit eine automatisierte Au-
30 thentifizierung und Verbindungsaufbau erfolgen, ohne dass das lokale Netzwerk mit dem Internet verbunden sein muss und ohne dass ein Administrator in den Vorgang eingreifen muss.

Gemäß dem zweiten Ausführungsbeispiel kann eine lokale PKI für eine M2M (Machine-to-Machine) Kommunikation basierend auf einem mTLS (Mutual Transport Layer Security) vorgesehen sein.

5 Gemäß einem Aspekt des zweiten Ausführungsbeispiels kann eine Rechteverwaltung der Kommunikation der IoT Knoten 110 vorgesehen sein. Somit kann festgelegt werden, welcher der IoT Knoten 110 Daten lesen kann, Daten modifizieren kann, neue Daten anlegen kann oder einen Server innerhalb des lokalen Netzwerkes 100 konfigurieren kann. Jeder IoT Knoten 110 kann ein Client Zertifikat aufweisen, in welchem dessen Berechtigungen abgelegt sind. Diese Berechtigungen können durch einen Server (als Server fungierende
10 IoT Knoten 110) überprüft werden.

Gemäß einem Aspekt der vorliegenden Erfindung kann das zweite Ausführungsbeispiel zur Maschine-zu-Maschine Kommunikation und/oder zur Kommunikation zwischen einer Maschine und einem menschlichen Nutzer oder zwischen zwei menschlichen Nutzern verwendet werden. Ein menschlicher Nutzer kann sich beispielsweise mittels eines Gerätes
15 (Secure Stick) unabhängig von dem verwendeten IoT Knoten 110 innerhalb der lokalen PKI Struktur identifizieren.

Gemäß einem Aspekt der vorliegenden Erfindung kann die lokale Root PKI Instanz einen IoT Knoten 110 darstellen. Somit kann ein derartiger IoT Knoten 110 die Überprüfung von anderen IoT Knoten 110 in dem lokalen Netzwerk 100 oder die Aufnahme von neuen IoT
20 Knoten 110 in das lokale Netzwerk 100 automatisiert überwachen.

Gemäß einem Aspekt der vorliegenden Erfindung können mehrere virtuelle lokale Netzwerke vorgesehen sein, welche sich auch überschneiden können, um mehrere Anwendungen in dem lokalen Netzwerk 100 ausführen zu können. Für jede Anwendung kann ein separater PKI Root verwendet werden. Für jedes PKI Root kann somit ein virtuelles lokales
25 Netzwerk 101, 102 vorgesehen werden. Dies ist vorteilhaft, weil somit eine Trennung der jeweiligen Anwendungen basierend auf den virtuellen lokalen Netzwerken 101, 102 ermöglicht wird.

Gemäß einem weiteren Aspekt der vorliegenden Erfindung kann ein Hinzufügen eines neuen Knotens zu einem virtuellen lokalen Netzwerk eines Verwaltungsknotens halb automatisch erfolgen. Der Verwaltungsknoten kann den Nutzer auf nicht zugeordnete Knoten
30 hinweisen. Der Nutzer kann entscheiden, ob ein derartiger Knoten ausgewählt werden soll

oder nicht. Nach Auswahl des neuen Knotens kann der Knoten durch den Verwaltungsknoten wie oben beschrieben automatisch zugeordnet oder ignoriert werden.

5 Gemäß einem Ausführungsbeispiel der Erfindung führt einer der IoT Knoten 110 einen Reset oder ein Rücksetzen durch, wenn er eine Reset-Aufforderung mittels eines speziellen Paketes erhält, das auf Medienzugriffsebene empfangen wurde. Ein derartiges Paket ist typischerweise ungültig, kann aber individuelle Informationen des Knotens enthalten. Vorteilhafterweise ist es in einem IP-Protokoll basierten lokalen Netzwerk nur dann möglich, derartige Pakete zum IoT Knoten zu senden, wenn der Benutzer direkt ohne Zwischenstationen wie Switches mit dem IoT Knoten verbunden ist. Dies rührt daher, weil derartige Pakete nicht von einem Switch weitergeleitet werden. Somit ist auf einfache Art und Weise sichergestellt, dass eine Reset- oder Rücksetz-Anforderung nur dann möglich ist, wenn der Benutzer auch einen tatsächlichen physischen Zugriff auf den Knoten besitzt. Beispielsweise bei einem Ethernet Netzwerk mit einem 100 Base T1 Kabel beträgt der Maximalabstand 15 m zum Knoten.

15 Somit kann erfindungsgemäß auf einen Verlust des auf dem Computer 130 gespeicherten Zertifikats reagiert werden. Dies kann beispielsweise erfolgen, wenn der Computer 130 defekt ist. Wenn kein Zugriff auf das benötigte Zertifikat mehr möglich ist, dann muss die lokale PKI Struktur neu aufgesetzt werden. Dies ist im Stand der Technik durch eine Betätigung eines Reset Knopfes an dem IoT Knoten oder durch die Übermittlung eines entsprechenden Reset Befehls (unverschlüsselt) möglich. Die Verwendung eines unverschlüsselten Reset Befehls ist jedoch aus Sicherheitsaspekten nicht gewünscht, da somit das lokale Netzwerk von einem nicht Autorisierten zurückgesetzt werden kann. Ferner ist die Verwendung eines Reset Knopfes an dem IoT Knoten mit weiteren Kosten verbunden, die erfindungsgemäß vermieden werden sollen.

25 Der IoT Knoten gemäß der Erfindung weist weder ein Display noch Bedienelemente noch einen Reset Knopf auf. Der IoT Knoten weist lediglich eine erste Schnittstelle zur Kommunikation mit dem Netzwerk 120 auf. Eine zweite Schnittstelle kann zur Kommunikation mit Geräten verwendet werden, welche an den IoT Knoten 110 gekoppelt sind.

30 Mit der erfindungsgemäßen Rücksetzfunktion kann sichergestellt werden, dass kein Angreifer über das Internet die IoT Knoten 110 in dem lokalen Netzwerk 100 zurücksetzen kann. Vielmehr muss der Befehl bzw. die Aufforderung für das Rücksetzen von einem Ge-

rät gesendet werden, welches physisch direkt über ein Netzkabel mit dem rückzusetzenden IoT Knoten 110 gekoppelt ist. Die erfindungsgemäße Rücksetzaufforderung stellt somit einen virtuellen Reset-Knopf dar.

Fig. 5 zeigt eine schematische Darstellung einer Rücksetzeinheit gemäß einem Ausführungsbeispiel der Erfindung. Die Rücksetzeinheit 300 weist eine interne Energieversorgung 310 beispielsweise in Form einer Batterie oder einer Akkumulatoreinheit auf. Die Rücksetzeinheit 300 weist eine erste Schnittstelle 301 beispielsweise zum Anschluss an ein Single Pair Ethernet Hybridkabel auf. Die Rücksetzeinheit 300 weist eine zweite Schnittstelle 302 in Form eines USB Ladeanschlusses auf. Über diesen USB Ladeanschluss 302 kann die Energieversorgung 310 aufgeladen werden. Mittels der Rücksetzeinheit 300, welche an einen IoT Knoten 110 angeschlossen werden kann oder in einem IoT Knoten vorgesehen sein kann, kann der IoT Knoten mittels der Rücksetzeinheit 300 zurückgesetzt werden. Dies kann beispielsweise dann erfolgen, wenn ungültige Zustände der Leitungen bei einer Single Pair Ethernet Hybridverbindung vorliegen. Ein Beispiel für derartige ungültige Zustände ist eine zu niedrige Versorgungsspannung bei gleichzeitiger Abwesenheit eines T1 Links. Der IoT Knoten 110 muss dann von dem Netzwerk 120 getrennt und mit der Rücksetzeinheit 300 verbunden werden. Dies erfordert wiederum einen physischen Zugriff auf den IoT Knoten 110. Hierbei wird das ursprüngliche beispielsweise Single Pair Ethernet Hybridkabel von dem Knoten IoT 120 entfernt und der Knoten wird an die Rücksetzeinheit 300 angeschlossen. Die Rücksetzeinheit 300 dient dann als Energieversorgung für den IoT Knoten 110 und kann das Rücksetzen initiieren. Durch die Rücksetzeinheit 300 werden dann alle während des Betriebes installierten/erzeugten zweiten Zertifikate und Schlüsselpaare sowie weitere Informationen auf dem IoT Knoten 110 gelöscht und der Knoten muss erneut vom Verwaltungsknoten mit einem Root-Zertifikat eingebunden werden. Hinsichtlich des Sicherheitsmerkmals „Erschleichen von Zugriffsrechten“ ist die Verwendung von auf dem IoT Knoten erzeugten 2. Schlüsselpaaren besonders vorteilhaft, da diese nach dem Rücksetzen nicht wieder hergestellt werden können. Ferner muss nach dem Rücksetzen stets ein erneutes Einbinden des IoT Knotens 110 in ein virtuelles lokales Netz erfolgen, wodurch der Betreiber des virtuellen lokalen Netzes stets Kenntnis von dem Rücksetzvorgang erlangt.

Durch das Rücksetzen gemäß der Erfindung können alle Schlüsselpaare des Knotens sowie Zertifikate gelöscht werden. Dies hat zur Folge, dass der IoT Knoten weder bei einem Server der lokalen PKI Struktur angemeldet werden kann, noch kann ein Client auf diesen zurückgesetzten IoT Knoten zugreifen. Damit kann sichergestellt werden, dass ein Firmware Reset oder eine sich dadurch ergebende Möglichkeit des unautorisierten Zugriffs auf

das lokale Netzwerk nicht unbemerkt erfolgen kann. Vielmehr muss der Knoten erneut in die Netzwerkkumgebung eingeführt werden.

5 Gemäß einem Aspekt der vorliegenden Erfindung wird ein Verfahren zur sicheren lokalen Kommunikation netzwerkfähiger IoT Knoten innerhalb eines lokalen Netzwerks vorgesehen. Eine Einrichtung oder Installation der netzwerkfähigen IoT Knoten kann unter Verwendung kryptographischer Verfahren und zwei kryptographischer Schlüsselpaare erfolgen. Hiermit kann eine anonyme Einrichtung einer gesicherten Kommunikation in einem lokalen Netzwerk erlaubt werden. Ein Schlüsselpaar kann während der Produktion der IoT Knoten oder während der Inbetriebnahme erzeugt werden. Die zwei Schlüsselpaare können durch
10 ein Zertifikat mit einer bei der Produktion vergebenen Netzwerkadresse, welche in jedem lokalen Netzwerk gültig ist, verifiziert werden.

Gemäß einem Aspekt der vorliegenden Erfindung kann die Echtheit eines IoT Knotens anhand von lokalen Adressinformationen (beispielsweise eines mdns Hostnamens) sowie eines gerätespezifischen privaten Schlüssels überprüft werden.

15 Gemäß einem Aspekt der vorliegenden Erfindung kann ein Reset der in dem lokalen Netzwerk vorgesehenen IoT Knoten oder IoT Geräte erfolgen, indem spezielle Pakete auf der Medienzugriffsebene an die IoT Knoten versandt werden. Dies ist vorteilhaft, weil damit Angriffe wie Denial of Services vermieden werden können.

20 Gemäß einem Aspekt der vorliegenden Erfindung kann eine Rücksetzeinheit in oder an einem IoT Knoten vorgesehen werden, welcher ohne Reset-Knopf auskommt. Ein Befehl zum Reset kann über eine erste Schnittstelle der Rücksetzeinheit erfolgen, welche mit einem Single Pair Ethernet Hybridkabel gekoppelt ist. Ein Reset kann durch Empfangen eines speziellen Paketes oder durch Erfassen von ungültigen Leitungszuständen erfolgen.

25 Gemäß einem Aspekt der vorliegenden Erfindung können die IoT Knoten netzwerkfähige Smart-Home Geräte oder Geräte einer Gebäudeautomatisierung darstellen.

Ansprüche

1. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100), das nur über einen Computer (130) zumindest zeitweise mit dem Internet (200) verbunden ist, wobei das lokale Netzwerk (100) ein Ethernet-Netzwerk oder eine Single Pair Ethernet-Netzwerk darstellt, wobei der IoT Knoten (110) oder das IoT Gerät Display-los und Bedienungselemente-frei ausgestaltet ist und eine erste Schnittstelle zur Kommunikation in dem lokalen Netzwerk (120) mit anderen IoT Knoten (110) oder dem Computer (130) aufweist, wobei jeder IoT Knoten (110) oder jedes IoT Gerät einen ersten öffentlichen kryptographischen Schlüssel und einen ersten privaten kryptographischen Schlüssel aufweist, wobei der erste private Schlüssel vorab abgelegt oder von dem IoT Knoten (110) oder dem IoT Gerät selber erzeugt wird, mit dem Schritt:

Authentifizierung von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) durch

- Senden einer Anfrage nach einem Root-Zertifikat (Z) durch den Computer (130) an einen Root-Zertifikat-Server (210) im Internet (200), der mindestens ein Root-Zertifikat (Z) eines Herstellers der IoT Knoten (110) oder der IoT Geräte aufweist,
 - Empfangen und Speichern des Root-Zertifikats (Z) durch den Computer (130), und
 - Überprüfen durch den Computer (130) anhand des empfangenen Root-Zertifikat (Z), ob die IoT Knoten (130) oder IoT Geräte originale und unveränderte Geräte sind, wobei das Root-Zertifikat (Z) dazu geeignet ist, den ersten öffentlichen Schlüssel der IoT Knoten (110) oder IoT Geräte mit einer eindeutigen ausschließlich im lokalen Netz gültigen Adressinformation des IoT Knotens (110) oder des IoT Gerätes zu verknüpfen,
- wobei der Computer (130) anhand des gespeicherten Root-Zertifikats (Z) überprüft, ob der öffentliche Schlüssel des IoT Knotens (110) oder des IoT Gerätes durch den Hersteller des IoT Knotens (110) oder des IoT Gerätes signiert ist,
- wobei der erste private Schlüssel des IoT Knotens (110) oder des IoT Gerätes basierend auf einem kryptografischen Verfahren überprüft wird.

2. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) nach Anspruch 1, wobei
- der Computer (130) nach Empfang des Root-Zertifikats (Z) von dem Root-Zertifikat-Servers (210) die Verbindung mit dem Internet (200) trennen kann, bevor die Prüfung der IoT Knoten (110) oder des IoT Gerätes erfolgt.

3. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) nach Anspruch 1 oder 2, wobei
jeder IoT Knoten (110) oder jedes IoT Gerät einen lokalen und eindeutigen Hostnamen, insbesondere eine IPv6 link local Adresse oder einen Multicast Domain Name System mDNS Netzwerknamen, aufweist.
4. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) nach einem der Ansprüche 1 bis 3, ferner mit den Schritten:
Einbinden von IoT Knoten (110) oder IoT Geräten in ein virtuelles lokales Netzwerk (101, 102) in Form einer lokalen Public-Key-Infrastruktur,
wobei jedem dieser IoT Knoten (110) oder IoT Geräten ein zweites kryptografisches Schlüsselpaar zugeordnet ist.
5. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) nach einem der Ansprüche 1 bis 4, ferner mit den Schritten:
Rücksetzen eines IoT Knotens (110) oder eines IoT Gerätes mittels einer Rücksetzeinheit (300), welche eine erste Schnittstelle (301) aufweist, welche dazu ausgestaltet ist, an ein Single Pair Ethernet Hybridkabel angeschlossen zu werden, wobei die Rücksetzeinheit (300) den IoT Knoten (110) oder das IoT Gerät zurücksetzt, wenn ungültige Zustände auf der Single Pair Ethernet Hybridleitung vorhanden sind.
6. Verfahren zur Kommunikation von IoT Knoten (110) oder IoT Geräten in einem lokalen Netzwerk (100) nach einem der Ansprüche 1 bis 5, wobei
mindestens einer der IoT Knoten (110) oder eines der IoT Geräte ein Client-Zertifikat aufweist, in welchem Nutzungsrechte, insbesondere Lese- und/oder Schreibrechte, des IoT Knotens (110) oder des IoT Gerätes gespeichert sind.
7. Lokales Internet-of-Things IoT Netzwerk (100) mit
einer Mehrzahl von IoT Knoten (110) oder IoT Geräten, welche Display-los und Bedienungselemente-frei ausgestaltet sind und jeweils eine erste Schnittstelle zur Kommunikation in dem lokalen Netzwerk (120) mit anderen IoT Knoten (110) oder einem Computer (130) in dem lokalen Netzwerk aufweisen,
mindestens einem Computer (130), der zumindest zeitweise mit dem Internet (200) verbunden ist,
wobei jeder IoT Knoten (110) oder jedes IoT Gerät einen ersten öffentlichen kryptografischen Schlüssel und einen ersten privaten kryptografischen Schlüssel aufweist,

wobei der erste private Schlüssel vorab abgelegt oder von dem IoT Knoten (110) oder dem IoT Gerät selber erzeugt wird.

wobei der Computer (130) dazu ausgestaltet ist, IoT Knoten (110) oder IoT Geräte in einem lokalen Netzwerk (100) zu authentifizieren durch Senden einer Anfrage nach einem Root-Zertifikat (Z) durch den Computer (130) an einen Root-Zertifikat-Server (210) im Internet (200), der mindestens ein Root-Zertifikat (Z) eines Herstellers der IoT Knoten (110) oder der IoT Geräte aufweist, durch Empfangen und Speichern des Root-Zertifikats (Z) durch den Computer (130) und durch Überprüfen, durch den Computer (130) anhand des empfangenen Root-Zertifikats (Z), ob die IoT Knoten (130) oder IoT Geräte originale und unveränderte Geräte sind, wobei das Root-Zertifikat (Z) dazu geeignet ist, den ersten öffentlichen Schlüssel der IoT Knoten (110) oder IoT Geräte mit einer eindeutigen ausschließlich lokal gültigen Adressinformation des IoT Knotens (110) oder des IoT Gerätes zu verknüpfen,

wobei der Computer (130) dazu ausgestaltet ist, anhand des gespeicherten Root-Zertifikats (Z) zu überprüfen, ob der erste öffentliche Schlüssel des IoT Knotens (110) oder des IoT Gerätes durch den Hersteller des IoT Knotens (110) oder des IoT Gerätes signiert ist,

wobei der erste private Schlüssel des IoT Knotens (110) oder des IoT Gerätes basierend auf einem kryptografischen Verfahren überprüft wird.

8. Lokales Internet-of-Things IoT Netzwerk nach Anspruch 7, ferner mit mindestens einer Rücksetzeinheit (300), welche eine erste Schnittstelle (301) aufweist, mittels welcher die Rücksetzeinheit (300) an eine Single Pair Ethernet Hybridleitung koppelbar ist,

wobei die Rücksetzeinheit (300) dazu ausgestaltet ist, einen angeschlossenen IoT Knoten (110) oder ein angeschlossenes IoT Gerät zurückzusetzen, wenn ungültige Zustände auf der Single Pair Ethernet Hybridleitung vorhanden sind.