(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 105 746 A1** 2014.12.04

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2013 105 746.2**
(22) Anmeldetag: **04.06.2013**
(43) Offenlegungstag: **04.12.2014**

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

(71) Anmelder:
Airbus Defence and Space GmbH, 85521 Ottobrunn, DE

(74) Vertreter:
Flügel Preissner Kastel Schober Patentanwälte PartG mbB, 80335 München, DE

(72) Erfinder:
Kubisch, Martin, Dr., 80469 München, DE

(56) Ermittelter Stand der Technik:

DE 10 2010 021 256 A1
US 2006 / 0 168 647 A1
WO 2013/ 013 243 A1

NFC FORUM, BLUETOOTH SPECIAL INTEREST GROUP: Bluetooth Secure Simple Pairing Using NFC - Application Document. 18.10.2011. URL: http://www.nfc-forum.org/resources/AppDocs/NFCForum_AD_BTSSP_1_0.pdf [abgerufen am 27.05.2013]

SWOBODA, J.; SPITZ, S.; PRAMATEFTAKIS, M.: Kryptographie und IT-Sicherheit. 1. Auflage. Wiesbaden : Vieweg + Teubner, 2008. Titelseite + Impressum + Seite 202. - ISBN 978-3-8348-0248-4

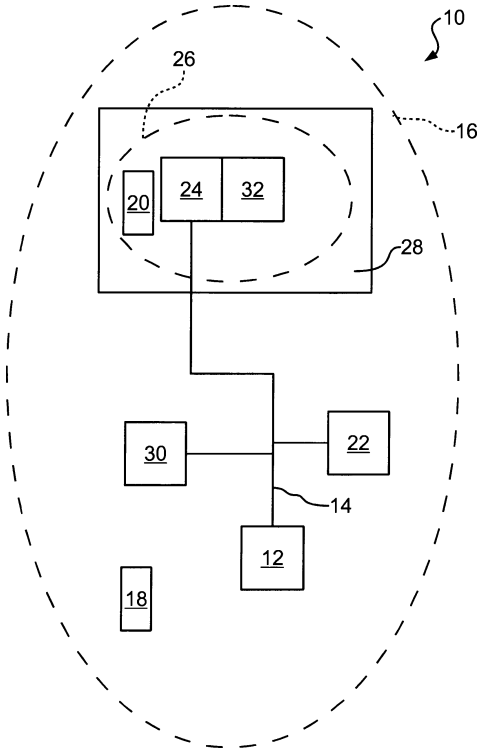
WARD Chris: InstaWifi-Connect to Wi-Fi using NFC or QR code. 14. Juni 2012. URL: http://blog.clove.co.uk/2012/06/14/instawificonnect-to-wi-fi-using-nfc-or-qr-code [abgerufen am 24.05.2013]

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Kommunikationssystem mit Zugangskontrolle sowie Verfahren zur Zugangsgewährung in einem Kommunikationssystem**

(57) Zusammenfassung: Ein Kommunikationssystem (10) weist eine erste drahtlose Kommunikationseinrichtung (12) zur Bereitstellung eines Kommunikationszugangs für eine mobile Rechnereinrichtung (18, 20) in einem ersten Kommunikationsbereich (16) auf. Die erste drahtlose Kommunikationseinrichtung (12) weist eine Zugangskontrolleinrichtung zur Zugangsgewährung aufgrund einer der mobilen Rechnereinrichtung (18, 20) bekannten Authentifizierungsinformation auf. Zur Bereitstellung der Authentifizierungsinformation für die mobile Rechnereinrichtung (18, 20) ist eine zweite Kommunikationseinrichtung (24) vorgesehen. Darüber hinaus betrifft die Erfindung ein Verfahren zur Zugangsgewährung, das mit dem oben genannten Kommunikationssystem (10) Durchführbar ist sowie ein Wartungssystem und/oder ein Luftfahrzeug mit einem derartigen Kommunikationssystem (10).



Beschreibung

[0001] Die Erfindung betrifft ein Kommunikationssystem mit einer ersten drahtlosen Kommunikationseinrichtung zur Bereitstellung eines Kommunikationszugangs für eine mobile Rechnereinrichtung in einem ersten Kommunikationsbereich. Die erste drahtlose Kommunikationseinrichtung weist eine Zugangskontrolleinrichtung zur Zugangsgewährung aufgrund einer der mobilen Rechnereinrichtung bekannten Authentifizierungsinformation auf. Darüber hinaus betrifft die Erfindung ein Verfahren zur Zugangsgewährung zu einem derartigen Kommunikationssystem, wobei eine Authentifizierungsinformation von einer mobilen Rechnereinrichtung empfangen, diese geprüft und, sofern die Authentifizierungsinformation korrekt ist, der Zugang zu dem Kommunikationssystem gewährt wird. Die Erfindung betrifft auch ein Luftfahrzeug und/oder ein Wartungssystem mit einem derartigen Kommunikationssystem und/oder zur Durchführung des Verfahrens.

[0002] Externe Wartungsgeräte/Rechnereinrichtungen zur Wartung von mobilen und immobilen Instanzen müssen an das zu wartende System angeschlossen werden. Dabei soll sichergestellt werden, dass der Zugriff autorisiert ist. Herkömmlicherweise wird dies dadurch erreicht, dass der Anschluss an das zu wartende System in einem geschützten und zugriffsbeschränkten Bereich stattfindet (Keller, Cockpit). Die Verwendung von drahtloser Umgebungskommunikation (WLAN, ZigBee) vereinfacht zwar das Anschließen des externen Wartungsgeräts, hebt jedoch die inhärente Kombination von Anschlussort und Zugriffsbeschränkung auf.

[0003] Als Authentifizierungsverfahren von Geräten an einem drahtlosen Netzwerk sind beispielsweise WPA2 und der Radius-Standard (802.1X) bekannt. Die meisten Authentifizierungsverfahren beruhen darauf, dass einer drahtlos kommunizierenden Rechnereinrichtung eine geheime Authentifizierungsinformation bekannt ist.

[0004] Die Erfindung beruht auf der Aufgabe, ein Kommunikationssystem der eingangs genannten Art derart weiterzubilden, dass eine Authentifizierungsinformation sicher von dem Kommunikationssystem an die Rechnereinrichtung übermittelt werden kann.

[0005] Die Aufgabe wird durch ein Kommunikationssystem gemäß Patentanspruch 1 gelöst, das eine zweite Kommunikationseinrichtung zur Bereitstellung der Authentifizierungsinformation für die mobile Rechnereinrichtung aufweist.

[0006] Ein derartiges Kommunikationssystem erlaubt es, die zweite Kommunikationseinrichtung in einem geschützten Bereich anzuordnen, so dass nur Rechnereinrichtungen die Authentifizierungsinformation erhalten, die Zugang zu diesem geschützten Bereich haben. Auf Seiten eines Bedieners der mobilen Rechnereinrichtung ist keine Eingabe von Authentifizierungsinformationen an der mobilen Rechnereinrichtung notwendig, wodurch Bedienerfehler reduziert werden.

[0007] Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche 2 bis 7.

[0008] Die zweite Kommunikationseinrichtung kann eine drahtlose Kommunikationseinrichtung sein, wobei die zweite Kommunikationseinrichtung einen zweiten Kommunikationsbereich aufweist, der kleiner ist als der erste Kommunikationsbereich. Vorteilhaft ist eine Sendeleistung der zweiten Kommunikationseinrichtung gegenüber der Sendeleistung der ersten Kommunikationseinrichtung reduziert. Dadurch muss die mobile Rechnereinrichtung zum Empfang der Authentifizierungsinformationen in einem vergleichsweise eng begrenzten Bereich angeordnet sein.

[0009] Die zweite Kommunikationseinrichtung kann drahtgebunden sein. Ein Anschluss der mobilen Rechnereinrichtung und ein Erhalten der Authentifizierungsinformationen ist somit nur an einem einfach zu schützenden physischen Zugangsort möglich.

[0010] Das Kommunikationssystem kann einen Authentifizierungsinformationsspeicher zur Aufnahme gültiger Authentifizierungsinformationen aufweisen, der von der ersten und der zweiten Kommunikationseinrichtung auslesbar ist. Dadurch kann die zweite Kommunikationseinrichtung aktuelle Authentifizierungsinformationen bereitstellen, die von der ersten Kommunikationseinrichtung beziehungsweise deren Zugangskontrolleinrichtung akzeptiert werden.

[0011] Der zweite Kommunikationsbereich geht vorteilhafterweise nicht über einen zugangsgesicherten Raum hinaus. Somit ist die physische Anwesenheit der mobilen Rechnereinrichtung in dem Raum notwendig. Dadurch lässt sich einfach nachvollziehen, welche Rechnereinrichtungen die Zugangsberechtigung erhalten.

[0012] Das Kommunikationssystem kann eine Terminaleinrichtung zur Identifikation eines Bedieners aufweisen. Dadurch ist es möglich, eine Two-Factor-Authentifizierung durchzuführen, beispielsweise indem neben der Anwesenheit der mobilen Rechnereinrichtung eine PIN-Eingabe oder eine Identifikationskarte verlangt wird.

[0013] Die Aufgabe wird darüber hinaus durch ein Verfahren nach Anspruch 8 gelöst, wobei dem eingangs genannten Verfahren der Schritt Übermitteln der Authentifizierungsinformationen mittels einer zweiten Kommunikationseinrichtung hinzugefügt wird.

[0014] Vorteilhafte Ausgestaltungen des Verfahrens sind Gegenstand der Unteransprüche 9 bis 12.

[0015] Es kann vorgesehen sein, dass ein zweiter Kommunikationsbereich der zweiten Kommunikationseinrichtung derart eingestellt wird, dass der zweite Kommunikationsbereich kleiner ist als der erste Kommunikationsbereich. Dadurch wird die Möglichkeit des Erhalts der Authentifizierungsinformationen auf einen physisch begrenzten Bereich beschränkt.

[0016] Darüber hinaus kann vorgesehen sein, dass die Authentifizierungsinformation erst nach dem Nachweis einer Zugangsberechtigung mittels einer Terminaleinrichtung übermittelt wird. Die Zugangsberechtigung kann durch Eingabe eines persönlichen Identifikationscode an der Terminaleinrichtung und/oder durch Einlesen von Daten einer Identifikationskarte durch die Terminaleinrichtung nachgewiesen werden. Durch eine derartige Two-Factor-Authentifizierung wird die Sicherheit des Kommunikationssystems erhöht.

[0017] Die Aufgabe wird ebenfalls durch ein Luftfahrzeug mit einem derartigen Kommunikationssystem sowie mit einem zur Durchführung des oben genannten Verfahrens geeigneten Kommunikationssystem gelöst.

[0018] Die Erfindung wird nachfolgend anhand von Ausführungsbeispielen näher erläutert, die in den beigefügten Figuren schematisch dargestellt sind. Im Einzelnen zeigen:

[0019] **Fig.** 1 eine Übersicht über eine erste Ausführungsform der vorliegenden Erfindung;

[0020] **Fig.** 2 eine Übersicht über eine zweite Ausführungsform der vorliegenden Erfindung und

[0021] **Fig.** 3 die Anordnung von Komponenten der zweiten Ausführungsform.

[0022] D1 zeigt ein Kommunikationssystem **10** mit einer ersten Kommunikationseinrichtung **12**. Die erste Kommunikationseinrichtung **12** stellt einen drahtlosen Kommunikationszugang zu einem Netzwerk **14** bereit. An das Netzwerk **14** sind verschiedene Rechnersysteme anschließbar, die unterschiedliche Funktionen erfüllen können.

[0023] Die erste Kommunikationseinrichtung **12**, die als WLAN-Accesspoint ausgebildet ist, weist einen ersten Kommunikationsbereich **16** auf, in dem mobile Rechnereinrichtungen **18**, **20** mit ihr kommunizieren können. Der erste Kommunikationsbereich **16** ist in dem vorliegenden Fall durch die Sende- und Empfangsleistung der ersten Kommunikationseinrichtung **12** sowie der mobilen Rechnereinrichtungen **18**, **20** begrenzt.

[0024] Die erste Kommunikationseinrichtung **12** weist eine Zugangskontrolleinrichtung (nicht gezeigt) auf, die darüber entscheidet, ob eine mobile Rechnereinrichtung **18**, **20** Zugang zu der ersten Kommunikationseinrichtung **12** erhält. Eine derartige Zugangskontrolleinrichtung kann auf verschiedene Arten implementiert werden. In dem vorliegenden Fall muss der mobilen Rechnereinrichtung **18**, **20** eine Authentifizierungsinformation bekannt sein, die zur Verschlüsselung einer Datenübertragung zwischen der mobilen Rechnereinrichtung **18**, **20** und der ersten Kommunikationseinrichtung **12** dient. In dem Kontext einer WPA2-Verschlüsselung ist diese Authentifizierungsinformation ein Zertifikat oder ein Passwort.

[0025] Sofern der mobilen Rechnereinrichtung **18**, **20** das Zertifikat oder das Passwort nicht bekannt sind, kann diese keine korrekt verschlüsselten Daten an die erste Kommunikationseinrichtung **12** versenden oder von ihr empfangen. Dadurch wird effektiv der Zugang zu der ersten Kommunikationseinrichtung **12** verweigert.

[0026] Es existiert eine Vielzahl von weiteren Verfahren zur Authentifizierung, die jeweils darauf beruhen, dass der mobilen Rechnereinrichtung **18**, **20**, wenn sie zum Zugriff berechtigt ist, eine Authentifizierungsinformation bekannt ist.

[0027] Das Kommunikationssystem **10** weist einen Authentifizierungsinformationsspeicher **22** zur Aufnahme gültiger Authentifizierungsinformationen auf. Mittels des Netzwerks **14** können angeschlossene Kommunikationseinrichtungen **12** auf den Authentifizierungsinformationsspeicher **22** zugreifen und dadurch ermitteln, welche Authentifizierungsinformationen gültig sind.

[0028] In bestimmten Situationen soll einer mobilen Rechnereinrichtung **18**, **20** nicht permanent Zugriff auf die erste Kommunikationseinrichtung **12** gewährt werden. Dies ist beispielsweise bei Wartungssystemen der Fall, bei denen mobilen Diagnosegeräten nur für den Zeitraum der Wartung Zugriff gewährt werden soll, da sie zur Wartung unterschiedlicher Systeme verwendbar sein sollen. Für einen derartigen Wartungszeitraum wird eine temporäre Authentifizierungsinformation erzeugt, die der mobilen Rechnereinrichtung **18**, **20** übermittelt wird. Zur Erzeugung dieser temporären Authentifizierungsinformation weist das Kommunikationssystem **10** eine Authentifizierungsinformationserzeugungseinrichtung **30** auf. Die Authentifizierungsinformationserzeugungseinrichtung **30** erzeugt Authentifizierungsinformationen, die beispielsweise in dem Authentifizierungsinformationsspeicher **22** abgelegt werden.

[0029] Zum Zweck der Übermittlung der temporären Authentifizierungsinformation weist das Kommunikationssystem **10** eine zweite Kommunikationseinrich-

tung **24** mit einem zweiten Kommunikationsbereich **26** auf. Sofern sich die mobile Rechnereinrichtung **18**, **20** in dem zweiten Kommunikationsbereich **26** befindet, kann sie von der zweiten Kommunikationseinrichtung **24** die Authentifizierungsinformation für den Zugang zu der ersten Kommunikationseinrichtung **12** anfordern.

[0030] Damit diese temporäre Authentifizierungsinformation nur an mobile Rechnereinrichtungen **18**, **20** übermittelt wird, die tatsächlich an einer Wartung beteiligt sind, ist der zweite Kommunikationsbereich **26** kleiner als der erste Kommunikationsbereich **16** und in einem gesicherten Bereich **28** angeordnet, der nur für berechtigte Personen, insbesondere für Wartungspersonal, zugänglich ist. In einem Luftfahrzeug wäre ein geeigneter Bereich **28** das Cockpit.

[0031] Da sich die mobile Rechnereinrichtung **20** in dem gesicherten Bereich **28** und auch in dem zweiten Kommunikationsbereich **26** befindet, wird also angenommen, dass der Rechnereinrichtung **20** auch Zugriff auf die erste Kommunikationseinrichtung **12** gewährt werden soll. Die mobile Rechnereinrichtung **18**, die sich nicht in dem zweiten Kommunikationsbereich **26** befindet, kann die Authentifizierungsinformationen nicht anfordern, da sie Nachrichten von der zweiten Kommunikationseinrichtung **24** nicht empfangen kann.

[0032] Zusätzlich zu der Notwendigkeit, Zugang zu dem gesicherten Bereich **28** zu haben ist die Freigabe der Authentifizierungsinformation an eine Freischaltung durch eine Terminaleinrichtung **32** gekoppelt. Die Terminaleinrichtung **32** erwartet eine zusätzliche Identifikation, beispielsweise einen Pincode oder eine Mitarbeiter-Identifikationskarte. Zu diesem Zweck kann die Terminaleinrichtung **32** eine Tastatur und/oder einen Kartenleser aufweisen. Erst wenn diese zusätzliche Identifikation erfolgreich abgeschlossen ist, wird der mobilen Rechnereinrichtung **20** die Authentifizierungsinformation übermittelt.

[0033] Die Freigabe der Authentifizierungsinformation durch die Terminaleinrichtung **32** ist allerdings optional, so dass die Terminaleinrichtung **32** nicht unbedingt notwendig ist.

[0034] Drahtlose Systeme finden in der Luft- und Raumfahrt Anwendung, sind jedoch aufgrund der Sicherheitsanforderungen (Schutz vor unerlaubtem Eingriff) meistens lediglich als lesender Zugriff auf Messsysteme (Tyre pressure, High lift torque limiter) umgesetzt. In der Gebäudetechnik werden solche Systeme ebenfalls als Nur-Lesesysteme verwendet, beispielsweise zum Ablesen von Strom- und Heizunswerten.

[0035] Die Wartung und Instandhaltung von mobilen und immobilen Instanzen (z. B. Flugzeug, Auto, Zug, Häusern) können durch den Einsatz von drahtlosen Geräten vereinfacht werden. **Fig.** 2 stellt dies für die Wartung eines Flugzeugs **50** dar. Das Flugzeug **50** ist mit einer ersten Kommunikationseinrichtung in Form eines drahtlosen Anschlusspunkts **12** ausgestattet und ein Wartungsmechaniker kann mit Hilfe eines drahtlosen Geräts in Form einer mobilen Rechnereinrichtung **18** Statusabfragen oder Wartungsfunktionen von einer beliebigen Position aus – am oder im Flugzeug **50** – ausführen.

[0036] Er ist somit nicht mehr darauf angewiesen, den Status direkt an der Quelle abzulesen (z. B. Getriebe im Flügel) oder sich mit zusätzlichem Personal im Cockpit abzustimmen um Getriebe an- oder abzuschalten. **Fig.** 2 stellt den Zugriff eines drahtlosen Geräts **18** an den drahtlosen Anschlusspunkt **12** des Flugzeugs **50** z. B. per IEEE802.11 dar.

[0037] Herkömmlicherweise wird die exklusive und gesicherte Nutzung von Statusabfragen und Wartungsfunktionen dadurch erreicht, dass der Anschluss an das zu wartende System drahtgebunden in einem geschützten und zugriffsbeschränkten Bereich des Wartungsobjekts stattfindet (Anschluss eines Steckers im Keller, unter der Motorhaube oder in der Fahrerkabine). Die Verwendung von drahtlosen Geräten **18** hebt jedoch die inhärente Kombination von Anschlussort und Zugriffsbeschränkung auf.

[0038] Die Verwendung von drahtlosen Geräten **18** erfordert deshalb, dass nur autorisierte drahtlose Geräte **18** sich mit dem drahtlosen Anschlusspunkt **12** verbinden dürfen um Zugriff auf die Statusinformationen und Wartungsfunktionen des Wartungsobjekts zu haben. Dies darf auch nur für eine begrenzte Dauer (Wartungssession) möglich sein.

[0039] Die vorliegende Erfindung beruht darauf, das Vorhandensein eines zugriffsbeschränkten Bereichs **28** zu nutzen, um drahtlose Geräte **18** dort an einer zweiten Kommunikationseinrichtung in Form eines Autorisierungspunkts **24** mit drahtloser Nahfeldkommunikation zu autorisieren (z. B. NFC, RFID, Infrarot) und ihnen den Zugriff auf den drahtlosen Anschlusspunkt **12** für eine Wartungssession zu geben.

[0040] In einem Flugzeug kann der zugriffsbeschränkte Bereich z. B. das Cockpit **28** oder der Frachtraum sein. In **Fig.** 3 ist das Cockpit **28** als zugriffsbeschränkter Bereich mit drahtlosem Autorisierungspunkt **24** dargestellt.

[0041] Die mobile Rechnereinrichtung **18** bildet ein externes Wartungsgerät, das wie auch das zu wartende System jeweils mit zwei Arten drahtloser Schnittstellen ausgestattet ist. Eine Schnittstelle für das Nahfeld (zum Beispiel NFC, RFID) und eine (oder mehrere) drahtlose Schnittstellen für die drahtlose Umgebungskommunikation (zum Beispiel WLAN).

Die Nahfeldschnittstelle befindet sich nur in einem geschützten und zugriffsbeschränkten Bereich **28** (Cockpit, abgeschlossener Kellerraum, Auto Innenraum). Über die Nahfeldschnittstelle wird erst der Sitzungsschlüssel (”Session Key”) übertragen, der es dem externen Wartungsgerät **18** dann ermöglicht, über die drahtlose Umgebungskommunikation mit dem Wartungssystem in Kontakt zu treten.

[0042] Bevor das drahtlose Gerät **18** eine Verbindung mit dem drahtlosen Anschlusspunkt **12** herstellen kann, muss es über den Autorisierungspunkt **24** im zugriffsbeschränkten Bereich **28** den Schlüssel für die Wartungssession erfahren. Nach Ablauf der Wartungssession erklärt der drahtlose Anschlusspunkt **12** den Schlüssel für ungültig und beendet die Verbindung mit dem drahtlosen Gerät **18**. Erst nach einer erneuten Autorisierung und Erhalt eines neuen Schlüssels, kann das drahtlose Gerät **18** wieder auf die Steuerdaten und Wartungsfunktionen des Wartungsobjekts zugreifen.

[0043] Die Vorteile der vorliegenden Erfindung umfassen, dass das externe Wartungsgerät **18** nicht mehr ortsgebunden ist. Dadurch kann ein Servicetechniker Aktionen ausführen (beispielsweise eine Heizungspumpe starten) und gleichzeitig den Effekt an der weit entfernten Heizung beobachten.

[0044] Darüber hinaus ist keine aufwändige Konfiguration der Zugriffsberechtigungen der Umgebungskommunikation mehr notwendig.

[0045] Über die Nahfeldschnittstelle kann die Systemsicherheit durch ein Softwareupdate des externen Wartungsgeräts **18** wiederhergestellt werden.

[0046] In dem geschützten Bereich kann eine zusätzliche Sicherheitsvorrichtung, beispielsweise in Form einer Terminaleinrichtung **32**, beispielsweise in Form eines Eingabegerätes für einen PIN-Code oder eines Kartenlesers für eine Firmen-ID vorgesehen sein.

[0047] Der zweite Kommunikationsbereich **26** kann dadurch verkleinert werden, dass eine Sendeleistung der zweiten Kommunikationseinrichtung reduziert wird. Darüber hinaus ist es möglich, den zweiten Kommunikationsbereich **26** dadurch zu verändern, dass eine Antenne der zweiten Kommunikationseinrichtung **24** eine besondere Form aufweist oder dass Abschirmungseinrichtungen vorgesehen sind, die einen Sende- und/oder Empfangsbereich der zweiten Kommunikationseinrichtung **24** beschränken.

[0048] Die erste Kommunikationseinrichtung **12** kann nicht nur auf IEEE802.11 (WLAN), sondern auf einem beliebigen Funkstandard basieren (beispielsweise ZigBee oder Bluetooth).

[0049] Der Authentifizierungsinformationsspeicher **22** sowie die Authentifizierungsinformationserzeugungseinrichtung **30** sind als separate, mittels des Netzwerks **24** mit den Kommunikationseinrichtungen **12**, **24** verbundene Einrichtungen gezeigt. Es ist genauso möglich, den Authentifizierungsinformationsspeicher **22** und/oder die Authentifizierungsinformationserzeugungseinrichtung **30** als eine gemeinsame Einrichtung vorzusehen. Darüber hinaus können der Authentifizierungsinformationsspeicher **22** und/oder die Authentifizierungsinformationserzeugungseinrichtung **30** in eine der Kommunikationseinrichtungen **12**, **24** integriert sein.

[0050] Die Kommunikationseinrichtungen **12**, **24** sind in dem vorliegenden Ausführungsbeispiel separat ausgebildet, können jedoch in eine einzelne Kommunikationseinrichtung integriert sein.

[0051] Die zweite Kommunikationseinrichtung **24** kann außerhalb des ersten Kommunikationsbereichs **16** angeordnet sein.

[0052] Der Authentifizierungsinformationsspeicher **22** kann es vorsehen, dass Authentifizierungsinformationen nach Verstreichen einer bestimmten Zeit ungültig oder gelöscht werden. Darüber hinaus kann der Authentifizierungsinformationsspeicher **22** es vorsehen, dass temporäre, für eine Wartung erzeugte Authentifizierungsinformationen am Ende einer Wartung auf Befehl gelöscht werden können.

[0053] Die vorliegende Erfindung erlaubt es auf einfache Weise, eine Zugangskontrolle zu einem drahtlosen Netzwerk bereitzustellen, die einfach bedienbar und trotzdem zuverlässig ist.

Bezugszeichenliste

10	Kommunikationssystem
12	Erste Kommunikationseinrichtung
14	Netzwerk
16	Erster Kommunikationsbereich
18	Mobile Rechnereinrichtung
20	Mobile Rechnereinrichtung
22	Authentifizierungsinformationsspeicher
24	Zweite Kommunikationseinrichtung
26	Zweite Kommunikationsbereich
28	Gesicherter Bereich
30	Authentifizierungsinformationserzeugungseinrichtung
32	Terminaleinrichtung
50	Flugzeug

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Nicht-Patentliteratur

- Radius-Standard (802.1X) [0003]
- IEEE802.11 [0036]
- IEEE802.11 [0048]

Patentansprüche

1. Kommunikationssystem (**10**), aufweisend
eine erste drahtlose Kommunikationseinrichtung (**12**) zur Bereitstellung eines Kommunikationszugangs für eine mobile Rechnereinrichtung (**18**, **20**) in einem ersten Kommunikationsbereich (**16**), wobei die erste drahtlose Kommunikationseinrichtung (**12**) eine Zugangskontrolleinrichtung zur Zugangsgewährung aufgrund einer der mobilen Rechnereinrichtung (**18**, **20**) bekannten Authentifizierungsinformation aufweist,
gekennzeichnet durch
eine zweite Kommunikationseinrichtung (**24**) zur Bereitstellung der Authentifizierunginformation für die mobile Rechnereinrichtung (**18**, **20**).

2. Kommunikationssystem nach Anspruch 1, **dadurch gekennzeichnet,** dass die zweite Kommunikationseinrichtung (**24**) eine drahtlose Kommunikationseinrichtung ist, wobei die zweite Kommunikationseinrichtung (**24**) einen zweiten Kommunikationsbereich (**26**) aufweist, der kleiner ist als der erste Kommunikationsbereich (**16**).

3. Kommunikationssystem nach Anspruch 2, **dadurch gekennzeichnet,** dass eine Sendeleistung der zweiten Kommunikationseinrichtung (**24**) gegenüber einer Sendeleistung der ersten Kommunikationseinrichtung (**12**) reduziert ist.

4. Kommunikationseinrichtung nach Anspruch 1, **dadurch gekennzeichnet,** dass die zweite Kommunikationseinrichtung (**24**) drahtgebunden ist.

5. Kommunikationssystem nach einem der voranstehenden Ansprüche, **dadurch gekennzeichnet,** dass das Kommunikationssystem (**10**) einen Authentifizierungsinformationsspeicher (**22**) zur Aufnahme gültiger Authentifizierungsinformationen aufweist, der von der ersten und der zweiten Kommunikationseinrichtung (**12**, **24**) auslesbar ist.

6. Kommunikationssystem nach einem der voranstehenden Ansprüche, **dadurch gekennzeichnet,** dass der zweite Kommunikationsbereich (**46**) nicht über einen gesicherten Bereich (**28**) hinausgeht.

7. Kommunikationssystem nach einem der voranstehenden Ansprüche, **dadurch gekennzeichnet,** dass die zweite Kommunikationseinrichtung (**24**) eine Terminaleinrichtung (**32**) zur Identifikation eines Bedieners aufweist.

8. Verfahren zur Zugangsgewährung zu einem Kommunikationssystem (**10**), das eine erste drahtlose Kommunikationseinrichtung (**12**) sowie einen ersten Kommunikationsbereich (**16**) aufweist, mit den Schritten:
Empfangen einer Authentifizierungsinformation von einer mobilen Rechnereinrichtung (**18**, **20**);
Prüfen der Authentifizierungsinformation;
Gewähren des Zugangs zu dem Kommunikationssystem (**10**), sofern die Authentifizierungsinformation korrekt ist;
gekennzeichnet durch den Schritt
Übermitteln der Authentifizierungsinformation mittels einer zweiten Kommunikationseinrichtung (**24**).

9. Verfahren nach Anspruch 8, gekennzeichnet durch den Schritt Einstellen eines zweiten Kommunikationsbereichs (**26**) der zweiten Kommunikationseinrichtung (**24**) derart, dass der zweite Kommunikationsbereich (**26**) kleiner ist als der erste Kommunikationsbereich (**26**).

10. Verfahren nach Anspruch 8 oder 9, gekennzeichnet durch den Schritt:
Übermitteln der Authentifizierungsinformation, nachdem eine Zugangsberechtigung mittels einer Terminaleinrichtung (**32**) nachgewiesen wurde.

11. Verfahren nach Anspruch 10, gekennzeichnet durch den Schritt:
Nachweisen der Zugangsberechtigung durch Eingabe eines persönlichen Identifikationscodes an der Terminaleinrichtung (**32**).

12. Verfahren nach Anspruch 10, gekennzeichnet durch den Schritt:
Nachweisen der Zugangsberechtigung durch Einlesen von Daten einer Identifikationskarte durch die Terminaleinrichtung (**32**).

13. Luftfahrzeug mit einem Kommunikationssystem gemäß einem der Ansprüche 1 bis 7 und/oder zur Durchführung eines Verfahrens nach einem der Ansprüche 8 bis 12.

14. Wartungssystem mit einem Kommunikationssystem gemäß einem der Ansprüche 1 bis 7 und/oder zur Durchführung eines Verfahrens nach einem der Ansprüche 8 bis 12.

15. Luftfahrzeug mit einem Wartungssystem gemäß Anspruch 14.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

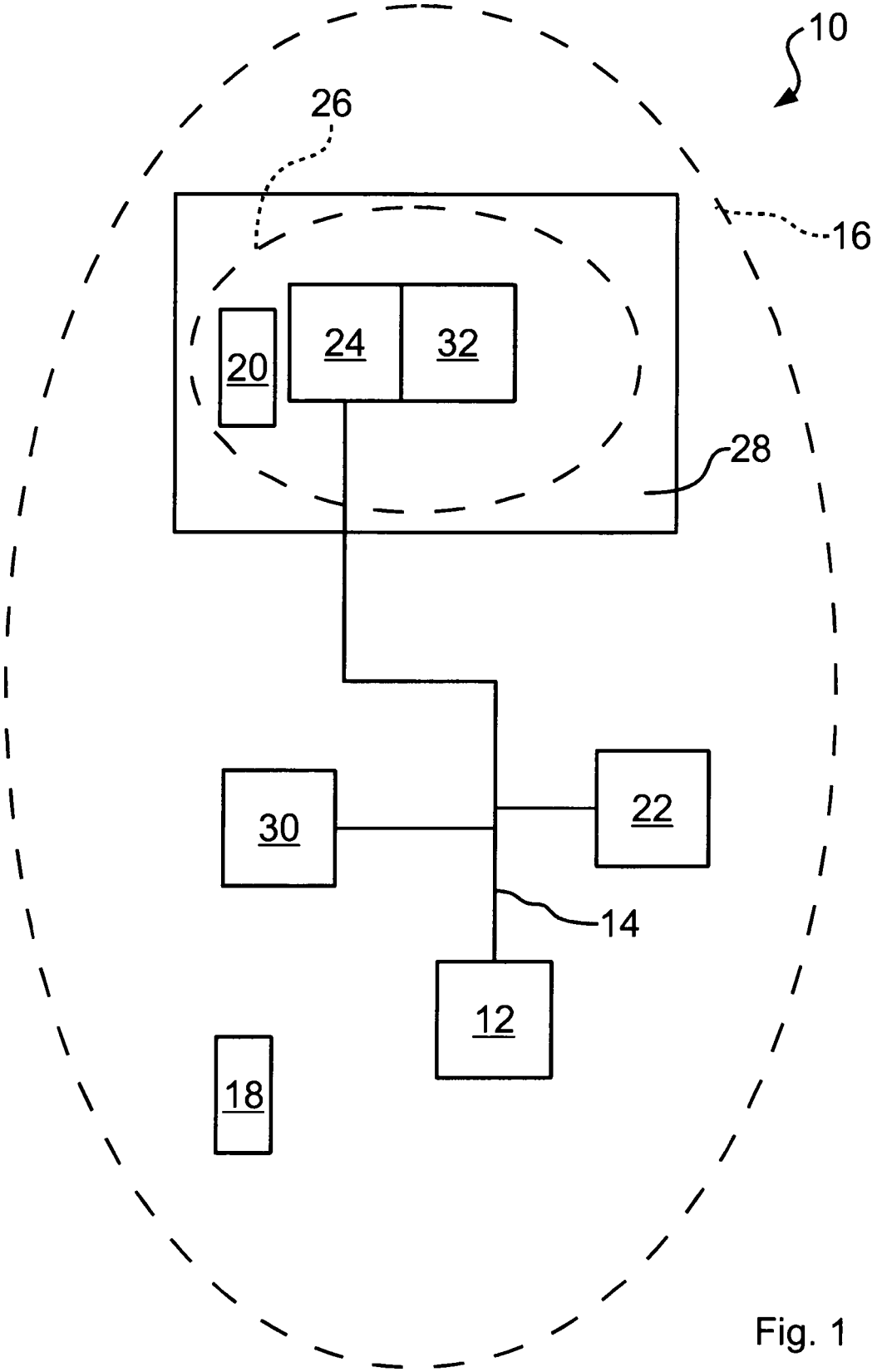


Fig. 1

FIG 2

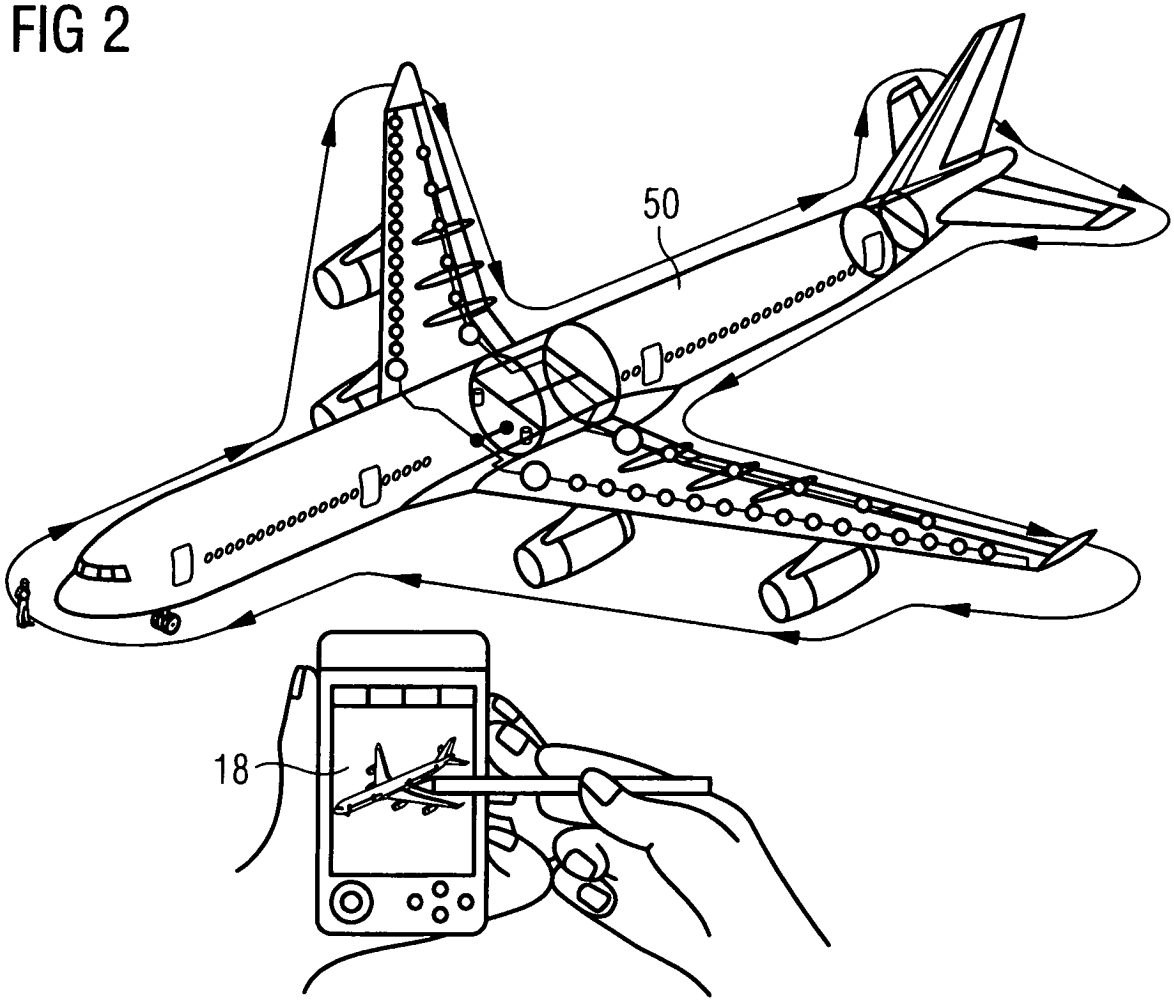


FIG 3