



(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2014 217 027.3**
 (22) Anmeldetag: **27.08.2014**
 (43) Offenlegungstag: **03.03.2016**

(51) Int Cl.: **G08C 17/02 (2006.01)**

(71) Anmelder:
Siemens Aktiengesellschaft, 80333 München, DE

(56) Ermittelter Stand der Technik:

(72) Erfinder:
Falk, Rainer, 85586 Poing, DE

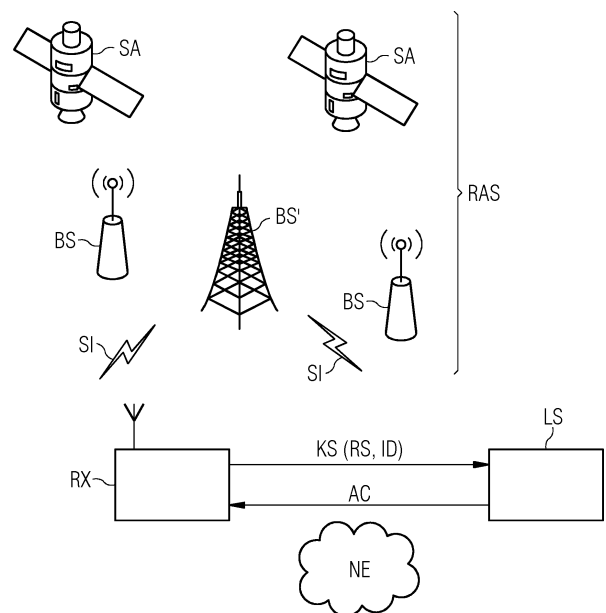
US	7 020 494	B2
US	2001 / 0 018 349	A1
US	2011 / 0 219 082	A1
US	2014 / 0 066 103	A1
US	2014 / 0 073 289	A1
US	2014 / 0 074 874	A1
EP	2 744 234	A1

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zum Freischalten von Funktionen in einem Funkempfänger**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Freischalten von Funktionen in einem Funkempfänger (RX). Der Funkempfänger (RX) erfasst einen Funksignalabschnitt (RS), indem er über eine vorbestimmte Zeitspanne ein oder mehrere, von ihm empfangene Funksignale (SI) eines Funksystems (RAS) aufzeichnet, wobei dem Funksignalabschnitt (RS) eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers (RX) bei Empfang des oder der Funksignale (SI) und/oder den Zeitpunkt des Empfangs des oder der Funksignale (SI) repräsentiert und welche aus dem Funksignalabschnitt (SI) ermittelbar ist. Der Funkempfänger (RX) wandelt diesen Funksignalabschnitt (RS) in ein Kommunikationssignal (KS), das über ein Kommunikationsnetz (NE) an einen Server (LS) übertragen wird. In dem Server (LS) wird dann mittels des Funksignalabschnitts (RS) in dem Kommunikationssignal (KS) bestimmt, ob die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt. Ist dies der Fall, sendet der Server (LS) einen Aktivierungscode (AC) über das Kommunikationsnetz (NE) an den Funkempfänger (RX), woraufhin ein Freischalten von einer oder mehreren Funktionen im Funkempfänger ausgelöst wird.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und ein System zum Freischalten von Funktionen in einem Funkempfänger.

[0002] Aus dem Stand der Technik ist es bekannt, mittels Geofencing die Nutzung eines Geräts auf einen bestimmten zulässigen geografischen Bereich bzw. ggf. auch einen zulässigen Zeitraum einzuschränken. Hierzu verfügt das Gerät über eine Positionsbestimmungsvorrichtung, welche Funksignale eines Funksystems auswertet, wie z.B. über einen GPS-Empfänger. Die über die Positionsbestimmungsvorrichtung ermittelte Position wird dabei im Gerät dahingehend geprüft, ob sich diese Position in einem vorbestimmten Gebiet befindet. Nur wenn dies der Fall ist, wird das Gerät als Ganzes bzw. bestimmte Funktionalitäten des Geräts freigeschaltet.

[0003] Mit Geofencing können z.B. verliehene Baumaschinen nur in zulässiger Weise genutzt werden. Weitere Anwendungen sind Mietwagen, Werttransporte und Geldausgabeautomaten. Auch kann mit Geofencing erreicht werden, dass ein Verschlüsselungsmodul nur in einem bestimmten Gebiet nutzbar ist. Da Funksignale und insbesondere GPS-Signale mit einfachen Mitteln fälschbar sind, kann Geofencing jedoch relativ einfach umgangen werden.

[0004] Ferner ist bei Satellitennavigationssystemen eine Empfänger-Architektur bekannt, bei der der Funkempfänger die Funksignale der Satelliten erfasst, digitalisiert und einen zeitlichen Funksignalabschnitt als sog. Radio Snippet (auch als Snippet bezeichnet) über ein Datenkommunikationsnetzwerk an einen Server zur weiteren Verarbeitung überträgt. Dabei wird die Positionsbestimmung nicht mehr im Funkempfänger selbst, sondern im Server durchgeführt, der dem Empfänger die ermittelte Position bereitstellt. Darüber hinaus gibt es Ansätze, wonach in einem satellitengestützten Navigationssystem kryptographisch geschützte Funksignale übertragen werden. Die in einem Funkempfänger empfangenen Signale werden dabei als Rohdaten erfasst und als Radio Snippet an ein sicheres Rechenzentrum über ein Datenkommunikationsnetzwerk weitergeleitet. Im sicheren Rechenzentrum erfolgt eine Weiterverarbeitung des kryptographisch geschützten Signals durch Ausführung von kryptographischen Operationen. Dadurch muss auf dem Funkempfänger keine sicherheitskritische Signalverarbeitung erfolgen. Der soeben beschriebene Ansatz wird z.B. im Kontext des Dienstes PRS (PRS = Public Regulated Service) des Satellitennavigationssystems Galileo durch das Projekt ULTRA verfolgt (siehe <http://www.ultra-prs.eu/>).

[0005] Aufgabe der Erfindung ist es, ein Verfahren und ein System zum Freischalten von Funktionen in einem Funkempfänger zu schaffen, welche zuverlässig

sig eine missbräuchliche Aktivierung von Funktionen verhindern, die nur in bestimmten Regionen bzw. zu bestimmten Zeitpunkten zulässig sind.

[0006] Das erfindungsgemäße Verfahren dient zum Freischalten von Funktionen in einem Funkempfänger. Der Begriff des Funkempfängers ist hier und im Folgenden derart zu verstehen, dass es sich um ein Gerät bzw. Objekt handelt, welches ein Funkmodul zum Empfang von Funksignalen beinhaltet, jedoch auch noch weitere Funktionen aufweisen kann, die nicht mit dem Funkempfang in unmittelbarem Zusammenhang stehen. Zum Beispiel kann ein Funkempfänger auch ein mobiles Objekt darstellen, wie etwa eine Baumaschine oder ein Kraftfahrzeug mit einem entsprechenden Funkmodul.

[0007] In einem Schritt a) des erfindungsgemäßen Verfahrens erfasst der Funkempfänger einen Funksignalabschnitt, indem er über eine vorbestimmte Zeitspanne ein oder mehrere, von ihm empfangene Funksignale eines Funksystems aufzeichnet. Dem Funksignalabschnitt ist dabei eine Orts- und/oder Zeitinformation zugeordnet, welche den Ort des Funkempfängers bei Empfang des oder der Funksignale und/oder den Zeitpunkt des Empfangs des oder der Funksignale im Funkempfänger repräsentiert und welche aus dem Funksignalabschnitt ermittelbar ist. Der Zeitpunkt des Empfangs kann einen beliebigen Zeitpunkt (inklusive Anfangs- und Endzeitpunkt) innerhalb des Funksignalabschnitts repräsentieren. Die vorbestimmte Zeitspanne der Aufzeichnung der Funksignale liegt die vorzugsweise im Bereich von wenigen Millisekunden bis zu einigen 10 Millisekunden.

[0008] Die durch den Funkempfänger empfangenen Funksignale können von einem beliebigen Funksystem stammen, sofern die Funksignale eine Lokalisation bzw. Zeitbestimmung ermöglichen. In einer besonders bevorzugten Variante stammen die Funksignale von einem Funksystem in der Form eines satellitengestützten Navigationssystems und der Funkempfänger enthält einen Satellitensignal-Empfänger für das satellitengestützte Navigationssystem. Nichtsdestotrotz kann das Funksystem ggf. auch ein lokales drahtloses Netzwerk, insbesondere ein WLAN-Netz, und/oder ein Mobilfunksystem und/oder ein Rundfunksystem umfassen. In diesem Fall enthält der Funkempfänger einen Empfänger für WLAN-Signale und/oder Mobilfunksignale und/oder Rundfunksignale.

[0009] In einem Schritt b) des erfindungsgemäßen Verfahrens wandelt der Funkempfänger den Funksignalabschnitt in ein Kommunikationssignal, welches den Funksignalabschnitt enthält. In einer Variante werden im Rahmen der Aufzeichnung der Funksignale diese zuerst digitalisiert und anschließend wird ein digitaler Funksignalabschnitt gebildet, der dann

in ein Format eines digitalen Kommunikationssignals gewandelt wird. In einer abgewandelten Variante wird der Funksignalabschnitt im Rahmen der Aufzeichnung als analoges Signal erfasst, welches dann in ein digitales Kommunikationssignal gewandelt wird. Der Funkempfänger sendet dieses Kommunikationssignal mittels einer geeigneten Schnittstelle über ein Kommunikationsnetz an einen Server. Je nach Ausführungsform kann das Kommunikationsnetz dabei unterschiedlich ausgestaltet sein. Insbesondere kann das Kommunikationsnetz ein drahtgebundenes und/oder drahtloses Netz sein. Zum Beispiel kann das Kommunikationsnetz das Internet und/oder ein Mobilfunknetz umfassen. Insbesondere muss das Kommunikationsnetz nicht mit dem Funksystem zusammenfallen, dessen Funksignale vom Funkempfänger aufgezeichnet werden.

[0010] In einem Schritt c) des erfindungsgemäßen Verfahrens wird das ausgesendete Kommunikationssignal über das Kommunikationsnetz von dem Server empfangen, der mittels des Funksignalabschnitts in dem Kommunikationssignal bestimmt, ob die dem Funksignalabschnitt zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt. Dieser Wertebereich kann z.B. in einer Datenbank hinterlegt sein, auf die der Server Zugriff hat. Der Begriff des zulässigen Wertebereichs ist weit zu verstehen. Insbesondere kann dieser Wertebereich einen kontinuierlichen Bereich oder ggf. auch eine Menge an zulässigen Werten darstellen.

[0011] In einem Schritt d) sendet der Server einen Aktivierungscode über das Kommunikationsnetz an den Funkempfänger, falls eine Anzahl von Kriterien erfüllt ist, wobei die Anzahl der Kriterien das Kriterium umfasst, dass die zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt. Die Definition des Kriteriums (eingeleitet mit dem Wort "dass") legt die Erfüllung des Kriteriums fest.

[0012] Schließlich wird in einem Schritt e) des erfindungsgemäßen Verfahrens der ausgesendete Aktivierungscode über das Kommunikationsnetz von dem Funkempfänger empfangen, woraufhin ein Freischalten von einer oder mehreren Funktionen im Funkempfänger ausgelöst wird. Ggf. kann die Freischaltung nur für eine vorbestimmte Zeitpanne bewirkt werden, wobei nach Ablauf der Zeitspanne die Freischaltung durch den Funkempfänger wieder gesperrt wird.

[0013] Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass die Prüfung der Zulässigkeit einer Orts- bzw. Zeitinformation, an welche die Verwendung von Funktionen in einem Funkempfänger gekoppelt ist, auf einen separaten Server verlagert wird, der mit dem Funkempfänger kommuniziert. Auf diese Weise werden lokale Manipulationen am Funkempfänger zum unbefugten Freischalten von Funk-

tionen verhindert. Vielmehr erfolgt die Freischaltung nur bei Empfang eines Aktivierungscode, der von außerhalb des Funkempfängers bereitgestellt wird.

[0014] In einer besonders bevorzugten Varianten des erfindungsgemäßen Verfahrens enthält das Kommunikationssignal ferner eine Identifikation des Funkempfängers, wobei der Server die Identifikation ausliest und bei der Bestimmung, ob die zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt, einen der Identifikation zugeordneten Wertebereich verwendet und/oder wobei der Server den Aktivierungscode in Abhängigkeit von der Identifikation des Funkempfängers bestimmt. Auf diese Weise kann die Freischaltung von Funktionen gerätespezifisch festgelegt werden.

[0015] In einer besonders bevorzugten Variante des erfindungsgemäßen Verfahrens berechnet der Server (direkt) aus dem Funksignalabschnitt, der in dem von ihm empfangenen Kommunikationssignal enthalten ist, die zugeordnete Orts- und/oder Zeitinformation. Anschließend vergleicht der Server die berechnete Orts- und/oder Zeitinformation mit dem zulässigen Wertebereich.

[0016] In einer weiteren Variante des erfindungsgemäßen Verfahrens vergleicht der Server den Funksignalabschnitt, der in dem von ihm empfangenen Kommunikationssignal enthalten ist, mit einer Menge von vorbestimmten Funksignalabschnitten, denen jeweils eine Orts- und/oder Zeitinformation in dem zulässigen Wertebereich zugeordnet ist. Bei ausreichender Übereinstimmung zwischen dem Funksignalabschnitt, der in dem vom Server empfangenen Kommunikationssignal enthalten ist, und einem vorbestimmten Funksignal aus der Menge von vorbestimmten Funksignalen wird bestimmt, dass die dem Funksignalabschnitt zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt. Dabei kann eine ausreichende Übereinstimmung zwischen den Funksignalabschnitten z.B. dadurch festgelegt sein, dass die Ähnlichkeit zwischen den Funksignalabschnitten ein vorbestimmtes Maß überschreitet. Entsprechende Verfahren zur Festlegung von Ähnlichkeiten zwischen Signalen sind dabei bekannt bzw. liegen im Rahmen von fachmännischem Handeln. Beispielsweise kann dazu eine Korrelation zwischen den Signalen durchgeführt werden.

[0017] In einer weiteren, besonders bevorzugten Ausführungsform enthält der Funksignalabschnitt kryptographisch geschützte Funksignale (z.B. verschlüsselte Funksignale). Dabei wird durch den Server im Rahmen der Bestimmung, ob die dem Funksignalabschnitt zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt, eine kryptographische Operation an dem Funksignal (z.B. eine Entschlüsselung oder eine Korrelation mit einem kryptographisch generierten Code, z.B. einem

kryptographischen Spreizcode) durchgeführt, welche den kryptographischen Schutz der Funksignale aufhebt (insbesondere mittels eines kryptographischen Schlüssels). Gemäß dieser Ausführungsform werden sicherheitskritische Funktionalitäten vom Funkempfänger hin zum Server verlagert, wodurch die Sicherheit des Verfahrens erhöht wird. Ferner können einfach aufgebaute und preiswerte Funkempfänger eingesetzt werden, die keine aufwändigen kryptographischen Operationen durchzuführen brauchen.

[0018] In einer weiteren Variante des erfindungsgemäßen Verfahrens umfasst die Anzahl von Kriterien neben dem Kriterium, dass die zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Bereich liegt, ein oder mehrere der folgenden Kriterien:

- das Kriterium, dass das Alter des Funksignalabschnitts gemäß der ihm zugeordneten Zeitinformation unterhalb eines vorbestimmten Schwellwerts liegt;
- das Kriterium, dass der Funksignalabschnitt eine oder mehrere Plausibilitätsbedingungen erfüllt, insbesondere in Bezug auf eine erwartete Dämpfung und/oder Verzerrung und/oder Signalstärke der in dem Funksignalabschnitt aufgezeichneten Funksignale.

[0019] Die entsprechende Definition des jeweiligen Kriteriums (eingeleitet mit dem Wort "dass") legt die Erfüllung des Kriteriums fest. Durch das obige Kriterium des Alters des Funksignalabschnitts wird sichergestellt, dass immer nur eine Freischaltung von Funktionen basierend auf aktuellen Funksignalen erfolgt. Durch das obige Kriterium betreffend die Plausibilitätsbedingungen wird die Sicherheit des Verfahrens gegenüber Manipulationen, z.B. durch gefälschte Funksignale, weiter erhöht. Entsprechende Verfahren zur Plausibilitätsprüfung von Signalen sind an sich aus dem Stand der Technik bekannt. Wie erwähnt, kann z.B. überprüft werden, ob eine erwartete Dämpfung bzw. Verzerrung in dem Funksignal auftritt, die bei Satelliten-Signalen z.B. bei Durchlaufen der Ionosphäre verursacht wird. Solche Dämpfungen bzw. Verzerrungen sind in gefälschten Satelliten-Signalen in der Regel nicht enthalten. Darüber hinaus kann auch die Plausibilität von Signalrauschen bzw. der absoluten Signalstärke oder der relativen Signalstärke der Funksignale überprüft werden.

[0020] Der im Rahmen des erfindungsgemäßen Verfahrens vom Server ausgesendete Aktivierungscode kann verschieden ausgestaltet sein. Insbesondere kann der Aktivierungscode einen numerischen und/oder alphanumerischen und/oder binären Code und/oder einen kryptographischen Schlüssel umfassen. Vorzugsweise weist der Aktivierungscode eine vorbestimmte Gültigkeitsdauer auf, welche vom Funkempfänger überprüft wird. Nur bei nicht abgelaufener Gültigkeitsdauer wird das Freischalten des oder der Funktionen im Funkempfänger ausgelöst. Vorzugs-

weise wird ferner nach Ablauf der Gültigkeitsdauer das Freischalten des oder der Funktionen durch den Funkempfänger gesperrt. Ggf. kann der Aktivierungscode auch eine Referenz auf den Funksignalabschnitt umfassen, der in Schritt c) von dem Server empfangen wurde, wobei nur im Falle, dass der Funkempfänger die Referenz einem von ihm ausgesendeten Funksignalabschnitt zuordnen kann, das Freischalten des oder der Funktionen im Funkempfänger ausgelöst wird.

[0021] Die im Funkempfänger freizuschaltende oder freizuschaltenden Funktionen können je nach Ausgestaltung unterschiedlich festgelegt sein. Insbesondere umfassen die Funktionen eine oder mehrere der folgenden Funktionen:

- die Wiedergabe eines Mediums durch den Funkempfänger, wie z.B. die Wiedergabe einer DVD oder einer Blu-ray-Disc;
- eine kryptographische Funktion eines kryptographischen Moduls in dem Funkempfänger, wie z.B. eines Crypto-Tokens, eines TPM-Moduls (TPM = Trusted Platform Modul) oder eines Hardware-Sicherheitsmoduls;
- die lokale Entschlüsselung von kryptographisch verschlüsselten Daten in dem Funkempfänger;
- die Aufhebung einer Bewegungssperre für den Funkempfänger, wie z.B. einer Wegfahrsperrung für ein mobiles Objekt;
- die Durchführung einer Konfiguration des Funkempfängers;
- die Funktion einer durch den Funkempfänger bewirkten entfernten Freischaltung von einer oder mehreren Funktionen in einem mit dem Funkempfänger kommunizierenden Gerät.

[0022] Die Freischaltung der Funktionen in dem mit dem Funkempfänger kommunizierenden Gerät kann die bereits oben genannten Funktionen betreffen, d.h. die Wiedergabe eines Mediums, die kryptographische Funktion eines kryptographischen Moduls, die Entschlüsselung von kryptographisch verschlüsselten Daten, die Aufhebung einer Bewegungssperre und die Durchführung einer Konfiguration. Diese Funktionen betreffen nunmehr jedoch nicht den Funkempfänger, sondern sie sind Funktionen des mit dem Funkempfänger kommunizierenden Geräts. Ggf. kann die freizuschaltende Funktion auch die Anzeige des Aktivierungscodes auf einem Display im Funkempfänger darstellen. In einem Anwendungsszenario kann der Aktivierungscode dann von einem Nutzer abgelesen werden und über eine entsprechende Benutzerschnittstelle am Funkempfänger eingegeben werden, um hierdurch weitergehende Funktionen im Funkempfänger freizuschalten.

[0023] Zur Erhöhung der Sicherheit des Verfahrens werden das Kommunikationssignal und/oder der Aktivierungscode vorzugsweise über eine kryptographisch geschützte Kommunikationsverbindung zwi-

schen dem Funkempfänger und dem Server über das Kommunikationsnetz übertragen (z.B. basierend auf IPsec, SSL, TLS).

[0024] Ein Aktivierungscode kann z.B. ein einzelnes Bit sein, durch das eine Freischaltung (bzw. keine Freischaltung) codiert ist. Vorzugsweise handelt es sich bei dem Aktivierungscode um eine Bitfolge, ein Passwort, eine PIN, einen Lizenzcode oder einen kryptographischen Schlüssel. In einer bevorzugten Variante wird der Aktivierungscode durch den Empfänger in einer kryptographischen Operation verwendet. So kann z.B. der Aktivierungscode oder ein Teil des Aktivierungscodes als kryptographischer Schlüssel oder als Schlüsselableitungsparameter verwendet werden, oder es kann dessen Gültigkeit mittels eines kryptographischen Schlüssels des Empfängers geprüft werden. Ein Aktivierungscode kann weitere Information umfassen, z.B. die Dauer der Freischaltung, den Startzeitpunkt der Freischaltung, einen Endzeitpunkt der Freischaltung, eine Angabe von freizuschaltenden Funktionen aus einer Menge von freischaltbaren Funktionen. Der Empfänger führt eine Freischaltung entsprechend der angegebenen Restriktionen durch. Das bedeutet, dass eine Freischaltung z.B. nur zeitlich begrenzt erfolgt bzw. dass nur eine Teilmenge von freischaltbaren Funktionen durch einen Aktivierungscode freigeschaltet wird.

[0025] Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein System aus Funkempfänger und Server, wobei der Funkempfänger und der Server zur Durchführung des erfindungsgemäßen Verfahrens bzw. einer oder mehrerer bevorzugter Varianten des erfindungsgemäßen Verfahrens eingerichtet sind.

[0026] Die Erfindung betrifft darüber hinaus einen Funkempfänger, der zur Verwendung in dem soeben beschriebenen System eingerichtet ist. Dieser Funkempfänger umfasst:

- ein Mittel zum Erfassen eines Funksignalabschnitts, indem über eine vorbestimmte Zeitspanne ein oder mehrere, von dem Funkempfänger empfangene Funksignale eines Funksystems aufgezeichnet werden, wobei dem Funksignalabschnitt eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers bei Empfang des oder der Funksignale und/oder den Zeitpunkt des Empfangs des oder der Funksignale repräsentiert und welche aus dem Funksignalabschnitt ermittelbar ist;
- ein Mittel zur Wandlung des Funksignalabschnitts in ein Kommunikationssignal, welche den Funksignalabschnitt enthält, sowie ein Mittel zum Aussenden dieses Kommunikationssignals über ein Kommunikationsnetz an einen Server;
- ein Mittel, um einen Aktivierungscode zu empfangen, der von dem Server über das Kommuni-

kationsnetz an den Funkempfänger ausgesendet wird, und um daraufhin ein Freischalten von einer oder mehrere Funktionen im Funkempfänger auszulösen.

[0027] Der Funkempfänger kann in der Form von entsprechenden Vorrichtungsmerkmalen auch solche Merkmale von Ausführungsformen des erfindungsgemäßen Verfahrens beinhalten, die den Funkempfänger betreffen.

[0028] Die Erfindung betrifft darüber hinaus einen Server, der zur Verwendung in dem oben beschriebenen System eingerichtet ist. Dabei umfasst der Server:

- ein Mittel zum Empfang eines von einem Funkempfänger ausgesendeten Kommunikationssignals über ein Kommunikationsnetz, wobei das Kommunikationssignal einen Funksignalabschnitt enthält, der eine Aufzeichnung von einem oder mehreren, von dem Funkempfänger empfangenen Funksignal eines Funksystems über eine vorbestimmte Zeitspanne ist, wobei dem Funksignalabschnitt eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers beim Empfang des oder der Funksignale und/oder den Zeitpunkt des Empfangs des oder der Funksignale repräsentiert und welche aus dem Funksignalabschnitt ermittelbar ist;
- ein Mittel, um mittels des Funksignalabschnitts in dem empfangenen Kommunikationssignal zu bestimmen, ob die dem Funksignalabschnitt zugeordnete Orts- und Zeitinformation in einem zulässigen Wertebereich liegt;
- ein Mittel, um einen Aktivierungscode über das Kommunikationsnetz an den Funkempfänger auszusenden, falls eine Anzahl von Kriterien erfüllt ist, wobei die Anzahl der Kriterien das Kriterium umfasst, dass die zugeordnete Orts- und Zeitinformation in dem zulässigen Wertebereich liegt.

[0029] Der Server kann in der Form von entsprechenden Vorrichtungsmerkmalen solche Merkmale von bevorzugten Ausführungsformen des erfindungsgemäßen Verfahrens enthalten, welche den Server betreffen.

[0030] Ein Ausführungsbeispiel der Erfindung wird nachfolgend detailliert anhand der beigefügten **Fig. 1** beschrieben, die schematisch die Freischaltung eines Funkempfängers gemäß einer Variante der Erfindung wiedergibt.

[0031] In dem Ausführungsbeispiel der **Fig. 1** wird eine Funkfunktionalität in dem Funkempfänger RX basierend auf dem geografischen Ort des Funkempfängers aktiviert. Alternativ oder zusätzlich kann ggf. auch eine Zeitinformation zum Freischalten von Funktionen im Funkempfänger berücksichtigt werden. Der Funkempfänger ist ein beliebiges Gerät

bzw. Objekt mit einer Empfangsfunktion für entsprechende Funksignale. Insbesondere kann der Funkempfänger ein mobiles Objekt, wie z.B. ein Fahrzeug oder eine Baumaschine, sein, für das verhindert werden soll, dass es in unzulässiger Weise außerhalb bestimmter Gebiete, z.B. außerhalb einer bestimmten Baustelle, eingesetzt werden.

[0032] Der Funkempfänger RX kommuniziert mit einem Funksystem RAS, bei dem es sich um ein beliebiges Funksystem handeln kann, dessen Funksignale eine Lokalisation des Funkempfänger RX ermöglichen. Beispielhaft ist durch die beiden Satelliten SA ein satellitengestütztes Funksystems, durch die Basisstationen BS eine WLAN-basiertes Funksystem und durch die Basisstation BS' ein Mobilfunksystem bzw. ein Rundfunksystem angedeutet. Nachfolgend wird eine Ausführungsform der Erfindung basierend auf einem Funkempfänger beschrieben, der die Signale eines satellitengestützten Navigationssystems, wie z.B. GPS, Glonass, Galileo und dergleichen, empfängt. In an sich bekannter Weise senden die Satelliten des Navigationssystems ein Funksignal aus, das von dem Funkempfänger RX empfangen wird. Anhand des aufmodulierten PRN-Codes des jeweiligen Satelliten kann die Laufzeit des Signals und damit eine Entfernungsinformation bestimmt werden. Wenn zumindest die Signale von vier Satelliten im Funkempfänger empfangen werden, kann die Position des Empfängers und die Zeit berechnet werden. In Varianten der Erfindung, bei denen lediglich eine Zeitinformation benötigt wird, reicht es aus, dass der Empfänger das Signal eines Satelliten empfängt.

[0033] In Fig. 1 sind die durch das Satelliten-Navigationssystem ausgesendeten Funksignale mit SI angedeutet. Es wird davon ausgegangen, dass der Empfänger RX die Signale von mindestens vier Satelliten empfängt, so dass hieraus seine geografische Position berechnet werden kann. In dem Empfänger RX ist die Freischaltung bestimmter Funktionen daran gekoppelt, ob sich der Funkempfänger in einem bestimmten geografischen Gebiet befindet. Herkömmlicherweise ermittelt der Empfänger selbst seine Position und leitet dann daraus ab, ob diese Position in dem vorbestimmten geografischen Gebiet liegt. Ist dies nicht der Fall, wird die Funktion nicht freigeschaltet. Im Unterschied hierzu wird erfindungsgemäß die Funktionalität der Positionsbestimmung des Empfängers sowie der Bestimmung, ob diese Position in einem vorbestimmten geografischen Gebiet liegt, durch einen separaten Lizenzserver LS vorgenommen. Dieser Lizenzserver kann über ein Kommunikationsnetz NE mit dem Funkempfänger RX kommunizieren. Das Kommunikationsnetz kann beliebig ausgestaltet sein, insbesondere kann das Netz ein Mobilfunknetz und/oder das Internet und dergleichen umfassen.

[0034] Der Funkempfänger RX zeichnet zunächst für eine vorbestimmte Zeitspanne die von ihm empfangenen Funksignale SI auf. Die Zeitspanne liegt im Bereich von wenigen Millisekunden. Die aufgezeichneten Satellitensignale werden im Folgenden auch als Funksignalabschnitte bzw. Snippets oder Radio Snippets bezeichnet und sind in Fig. 1 durch das Bezugszeichen RS repräsentiert. Diese Radio Snippets liegen zunächst in analoger Form vor. Zur Übermittlung an den Lizenzserver LS werden diese digitalisiert und zusammen mit einer eindeutigen Gerätidentifikation ID des Funkempfängers RX als digitales Kommunikationssignal KS an den Lizenzserver LS übermittelt.

[0035] In dem Lizenzserver LS erfolgt die Auswertung des Kommunikationssignals KS. Hierzu wird der Funksignalabschnitt RS aus dem Kommunikationssignal KS extrahiert und in an sich bekannter Weise weiterverarbeitet, um hieraus die geografische Position des Empfängers RX zu ermitteln. Anschließend wird diese Position mit einem zulässigen geografischen Gebiet verglichen, das für die Gerätidentifikation ID spezifisch ist. Das geografische Gebiet kann dabei in einer Datenbank des Lizenzservers hinterlegt sein, oder der Lizenzserver greift hierzu auf eine entfernte Datenbank zu. Falls die sich aus dem Radio Snippet RS ergebende Position in dem zulässigen Gebiet liegt, erzeugt der Lizenzserver einen für den Funkempfänger RS spezifischen Aktivierungscode AC. Diesen kann er z.B. aus einer Datenbank auslesen oder in geeigneter Weise mit einem Sicherheitsmodul berechnen. Der Aktivierungscode AC wird anschließend über das Kommunikationsnetz NE an den Funkempfänger RX übermittelt. Durch Empfang des Aktivierungscode wird dem Empfänger RX mitgeteilt, dass eine oder mehrere Funktionalitäten im Empfänger freigeschaltet werden können. Demzufolge wird die Freischaltung der Funktionalitäten durchgeführt.

[0036] Der vom Lizenzserver an den Funkempfänger RX übermittelte Aktivierungscode kann verschieden ausgestaltet sein. Zum Beispiel kann es sich um eine PIN oder einen anderweitigen Code handeln, um ein Sicherheitsmodul in dem Funkempfänger freizuschalten. Ebenso kann der Aktivierungscode ein kryptographischer Schlüssel sein, den der Funkempfänger z.B. zur Entschlüsselung von auf ihm gespeicherten Daten verwendet (z.B. Programmcode, Nutzerdaten und dergleichen). Ebenso kann der Aktivierungscode Konfigurationsdaten enthalten, mit denen der Funkempfänger anschließend konfiguriert wird.

[0037] In einem weiteren Anwendungsszenario enthält der Funkempfänger die Funktion eines sog. „Cognitive Radio“, bei dem der Funkempfänger adaptiv unbenutzte Frequenzbänder zur Datenübertragung nutzen kann. Dabei kann der Aktivierungscode z.B. angeben, welche Sendeleistung, welche Modulati-

onsverfahren und welche Frequenzbänder benutzt werden dürfen. Der Aktivierungscode bewirkt in diesem Sinne das Freischalten einer Funktion, mit der zu verwendende Frequenzbänder für ein Cognitive Radio festgelegt werden. Durch geeignete Festlegung des geografischen Bereichs, in dem diese Funktion freigeschaltet werden soll, kann berücksichtigt werden, dass in manchen Regionen bzw. Ländern Frequenzbänder für behördliche Zwecke vorgesehen sind und nicht anderweitig verwendet werden dürfen, wohingegen in anderen Regionen solche Bänder für Cognitive Radio nutzbar sind.

der Funkempfänger auch keine Mechanismen enthalten, um die Bestimmung seiner Position vor Manipulationen zu schützen.

[0038] In einer weiteren bevorzugten Ausführungsform ist eine feste oder ggf. auch vorgebbare Nutzungsdauer für den Aktivierungscode vorgesehen. Nach Ablauf der Nutzungsdauer wird der Code vom Funkempfänger gesperrt bzw. gelöscht. Auch kann der Aktivierungscode eine Information über seine Gültigkeitsdauer umfassen. Durch Wiederholung des oben beschriebenen Verfahrens kann der Funkempfänger nach Ablauf der Gültigkeitsdauer über einen neuen Aktivierungscode wieder freigeschaltet werden bzw. eine Sperrung von bestimmten Funktionen unterbleiben.

[0039] Die im Vorangegangenen beschriebenen Ausführungsformen des erfindungsgemäßen Verfahrens weisen eine Reihe von Vorteilen auf. Insbesondere wird eine unzulässige Nutzung des Funkempfängers zuverlässig dadurch verhindert, dass die Überprüfung, ob die Freischaltung einer Funktion im Funkempfänger zulässig ist, von einem separaten Lizenzserver vorgenommen wird. Eine erfolgreiche Manipulation mittels eines sog. GPS-Spoofers, der dem Funkempfänger eine andere als die tatsächliche Position vortäuscht, ist dabei wesentlich schwerer zu realisieren. Im Besonderen können in dem Lizenzserver aufwändige Verfahren realisiert werden, um GPS-Spoofers zu erkennen. Solche Verfahren können auf einem üblichen kommerziellen Funkempfänger nicht umgesetzt werden. Darüber hinaus kann in dem Lizenzserver auf einfache Weise abhängig von in der Praxis beobachteten Manipulationen die Auswertearithmetik zur Überprüfung eines Funksignalabschnitts angepasst werden, um künftige ähnliche Manipulationen zu verhindern.

[0040] Auch kann ein Lizenzserver unterschiedliche, ggf. nur aufwändig auswertbare Funksignalabschnitte verarbeiten. Insbesondere können durch ihn z.B. verschlüsselte Satellitennavigationssignale ausgewertet werden, die der Funkempfänger mangels Ressourcen selbst nicht entschlüsseln kann. Solche Satellitensignale sollen z.B. vom satellitengestützten Navigationsdienst Galileo PRS genutzt werden. Da der Funkempfänger selbst nicht seine eigene Position bestimmen muss, sondern nur ein Radio Snippet aufzeichnet und überträgt, ist der Realisierungsaufwand im Funkempfänger gering. Insbesondere muss

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

- <http://www.ultra-prs.eu/> [0004]

Patentansprüche

1. Verfahren zum Freischalten von Funktionen in einem Funkempfänger (RX), bei dem

a) der Funkempfänger (RX) einen Funksignalabschnitt (RS) erfasst, indem er über eine vorbestimmte Zeitspanne ein oder mehrere, von ihm empfangene Funksignale (SI) eines Funksystems (RAS) aufzeichnet, wobei dem Funksignalabschnitt (RS) eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers (RX) bei Empfang des oder der Funksignale (SI) und/oder den Zeitpunkt des Empfangs des oder der Funksignale (SI) repräsentiert und welche aus dem Funksignalabschnitt (SI) ermittelbar ist;

b) der Funkempfänger (RX) den Funksignalabschnitt (RS) in ein Kommunikationssignal (KS) wandelt, welches den Funksignalabschnitt (RS) enthält, und dieses Kommunikationssignal (KS) über ein Kommunikationsnetz (NE) an einen Server (LS) aussendet;

c) das ausgesendete Kommunikationssignal (KS) über das Kommunikationsnetz (NE) von dem Server (LS) empfangen wird, der mittels des Funksignalabschnitts (RS) in dem Kommunikationssignal (KS) bestimmt, ob die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt;

d) der Server (LS) einen Aktivierungscode (AC) über das Kommunikationsnetz (NE) an den Funkempfänger (RX) aussendet, falls eine Anzahl von Kriterien erfüllt ist, wobei die Anzahl der Kriterien das Kriterium umfasst, dass die zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt;

e) der ausgesendete Aktivierungscode (AC) über das Kommunikationsnetz (NE) von dem Funkempfänger (RX) empfangen wird, woraufhin ein Freischalten von einer oder mehreren Funktionen im Funkempfänger (RX) ausgelöst wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass das Funksystem (RAS) ein satellitengestütztes Navigationssystem umfasst und der Funkempfänger (RX) einen Satellitensignal-Empfänger für das satellitengestützte Navigationssystem enthält.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass das Funksystem (RAS) ein lokales drahtloses Netzwerk, insbesondere ein WLAN-Netzwerk, und/oder ein Mobilfunksystem und/oder ein Rundfunk-System umfasst und der Funkempfänger (RX) einen Empfänger für WLAN-Signale und/oder Mobilfunksignale und/oder Rundfunksignale enthält.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass das Kommunikationssignal (KS) ferner eine Identifikation (ID) des Funkempfängers (RX) enthält, wobei der Server (LS) die Identifikation ausliest und bei der Bestimmung, ob die zugeordnete Orts- und/oder Zeit-

information in dem zulässigen Wertebereich liegt, einen der Identifikation (ID) zugeordneten Wertebereich verwendet und/oder wobei der Server (23) den Aktivierungscode (AC) in Abhängigkeit von der Identifikation (ID) des Funkempfängers (RX).

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass der Server (LS) aus dem Funksignalabschnitt (RS), der in dem von ihm empfangenen Kommunikationssignal (KS) enthalten ist, die zugeordnete Orts- und/oder Zeitinformation berechnet und die berechnete Orts- und/oder Zeitinformation mit dem zulässigen Wertebereich vergleicht.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass der Server (LS) den Funksignalabschnitt (RS), der in dem von ihm empfangenen Kommunikationssignal (KS) enthalten ist, mit einer Menge von vorbestimmten Funksignalabschnitten vergleicht, denen jeweils eine Orts- und/oder Zeitinformation in dem zulässigen Wertebereich zugeordnet ist, wobei bei ausreichender Übereinstimmung zwischen dem Funksignalabschnitt (RS), der in dem von ihm empfangenen Kommunikationssignal (KS) enthalten ist, und einem vorbestimmten Funksignal bestimmt wird, dass die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass der Funksignalabschnitt (RS) kryptographisch geschützte Funksignale (SI) enthält und durch den Server (LS) im Rahmen der Bestimmung, ob die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt, eine kryptographische Operation an dem Funksignalabschnitt (RS) durchgeführt wird, welche den kryptographischen Schutz der Funksignale (SI) aufhebt.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Anzahl von Kriterien ferner ein oder mehrere der folgende Kriterien umfasst:

– das Kriterium, dass das Alter des Funksignalabschnitts (RS) gemäß der ihm zugeordneten Zeitinformation unterhalb eines vorbestimmten Schwellwerts liegt;

– das Kriterium, das der Funksignalabschnitt (RS) eine oder mehrere Plausibilitätsbedingungen erfüllt, insbesondere in Bezug auf eine erwartete Dämpfung und/oder Verzerrung und/oder Signalstärke der in dem Funksignalabschnitt (RS) aufgezeichneten Funksignale (SI).

9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass der Aktivierungscode (AC) eine vorbestimmte Gültigkeits-

dauer aufweist, wobei nur bei nicht abgelaufener Gültigkeitsdauer das Freischalten des oder der Funktionen im Funkempfänger (RX) ausgelöst wird, und/oder dass der Aktivierungscode (AC) eine Referenz auf den Funksignalabschnitt (RS) umfasst, der in Schritt c) von dem Server (LS) empfangen wurde, wobei nur im Falle, dass der Funkempfänger (RX) die Referenz einem von ihm zuvor ausgesendeten Funksignalabschnitt (RS) zuordnen kann, das Freischalten des oder der Funktionen im Funkempfänger (RX) ausgelöst wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die freizuschaltende oder freizuschaltenden Funktionen eine oder mehrere der folgenden Funktionen umfassen:

- die Wiedergabe eines Mediums durch den Funkempfänger (RX);
- eine kryptographische Funktion eines kryptographischen Moduls in dem Funkempfänger (RX);
- die Entschlüsselung von kryptographisch verschlüsselten Daten in dem Funkempfänger (RX);
- die Aufhebung einer Bewegungssperre für den Funkempfänger (RX);
- die Durchführung einer Konfiguration des Funkempfängers;
- die Funktion einer durch den Funkempfänger (RX) bewirkten entfernten Freischaltung von einer oder mehreren Funktionen in einem mit dem Funkempfänger (RX) kommunizierenden Gerät.

11. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass das Kommunikationssignal (KS) und/oder der Aktivierungscode (AC) über eine kryptographisch geschützte Kommunikationsverbindung zwischen dem Funkempfänger (RX) und dem Server (LS) über das Kommunikationsnetz (NE) übertragen werden.

12. System aus Funkempfänger (RX) und Server (LS), wobei der Funkempfänger (RX) und der Server (LS) zur Durchführung eines Verfahrens eingerichtet sind, bei dem:

- a) der Funkempfänger (RX) einen Funksignalabschnitt (RS) erfasst, indem er über eine vorbestimmte Zeitspanne ein oder mehrere, von ihm empfangene Funksignale (SI) eines Funksystems (RAS) aufzeichnet, wobei dem Funksignalabschnitt (RS) eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers (RX) bei Empfang des oder der Funksignale (SI) und/oder den Zeitpunkt des Empfangs des oder der Funksignale (SI) repräsentiert und welche aus dem Funksignalabschnitt (SI) ermittelbar ist;
- b) der Funkempfänger (RX) den Funksignalabschnitt (RS) in ein Kommunikationssignal (KS) wandelt, welches den Funksignalabschnitt (RS) enthält, und dieses Kommunikationssignal (KS) über ein Kommunikationsnetz (NE) an einen Server (LS) aussendet;

c) das ausgesendete Kommunikationssignal (KS) über das Kommunikationsnetz (NE) von dem Server (LS) empfangen wird, der mittels des Funksignalabschnitts (RS) in dem Kommunikationssignal (KS) bestimmt, ob die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt;

d) der Server (LS) einen Aktivierungscode (AC) über das Kommunikationsnetz (NE) an den Funkempfänger (RX) aussendet, falls eine Anzahl von Kriterien erfüllt ist, wobei die Anzahl der Kriterien das Kriterium umfasst, dass die zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt;

e) der ausgesendete Aktivierungscode (AC) über das Kommunikationsnetz (NE) von dem Funkempfänger (RX) empfangen wird, woraufhin ein Freischalten von einer oder mehreren Funktionen im Funkempfänger (RX) ausgelöst wird.

13. System nach Anspruch 12, **dadurch gekennzeichnet**, dass das System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 11 eingerichtet ist.

14. Funkempfänger (RX), der zur Verwendung in einem System nach Anspruch 12 oder 13 eingerichtet ist, wobei der Funkempfänger (RX) umfasst:

- ein Mittel zum Erfassen eines Funksignalabschnitts (RS), indem über eine vorbestimmte Zeitspanne ein oder mehrere, von dem Funkempfänger (RX) empfangene Funksignale (SI) eines Funksystems (RAS) aufgezeichnet werden, wobei dem Funksignalabschnitt (RS) eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers (RX) bei Empfang des oder der Funksignale (SI) und/oder den Zeitpunkt des Empfangs des oder der Funksignale (SI) repräsentiert und welche aus dem Funksignalabschnitt (SI) ermittelbar ist;
- ein Mittel zur Wandlung des Funksignalabschnitts (RS) in ein Kommunikationssignal (KS), welches den Funksignalabschnitt (RS) enthält, sowie ein Mittel zum Aussenden dieses Kommunikationssignals (KS) über ein Kommunikationsnetz (NE) an einen Server (LS);
- ein Mittel, um einen Aktivierungscode (AC) zu empfangen, der von dem Server (LS) über das Kommunikationsnetz (NE) an den Funkempfänger (RX) ausgesendet wird, und um daraufhin ein Freischalten von einer oder mehreren Funktionen im Funkempfänger (RX) auszulösen.

15. Server (LS), der zur Verwendung in einem System nach Anspruch 12 oder 13 eingerichtet ist, wobei der Server (LS) umfasst:

- ein Mittel zum Empfang eines von einem Funkempfänger (RX) ausgesendeten Kommunikationssignals (KS) über ein Kommunikationsnetz (NE), wobei das Kommunikationssignal (KS) einen Funksignalabschnitt (RS) enthält, der eine Aufzeichnung von einem oder mehreren, von dem Funkempfänger (RX)

empfangenen Funksignalen (SI) eines Funksystems (RAS) über eine vorbestimmte Zeitspanne ist, wobei dem Funksignalabschnitt (RS) eine Orts- und/oder Zeitinformation zugeordnet ist, welche den Ort des Funkempfängers (RX) bei Empfang des oder der Funksignale (RS) und/oder den Zeitpunkt des Empfangs des oder der Funksignale (SI) repräsentiert und welche aus dem Funksignalabschnitt (SI) ermittelbar ist;

– ein Mittel, um mittels des Funksignalabschnitts (RS) in dem empfangenen Kommunikationssignal (KS) zu bestimmen, ob die dem Funksignalabschnitt (RS) zugeordnete Orts- und/oder Zeitinformation in einem zulässigen Wertebereich liegt;

– ein Mittel, um einen Aktivierungscode (AC) über das Kommunikationsnetz (NE) an den Funkempfänger (RX) auszusenden, falls eine Anzahl von Kriterien erfüllt ist, wobei die Anzahl der Kriterien das Kriterium umfasst, dass die zugeordnete Orts- und/oder Zeitinformation in dem zulässigen Wertebereich liegt.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

