(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

BERICHTIGTE FASSUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. Oktober 2017 (19.10.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/178114 A9

(51) Internationale Patentklassifikation:
H04W 12/02 (2009.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01) *H04W 4/00* (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2017/000474

(22) Internationales Anmeldedatum:
11. April 2017 (11.04.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 004 426.8
12. April 2016 (12.04.2016) DE

(71) Anmelder: **GIESECKE+DEVRIENT MOBILE SECURITY GMBH** [DE/DE]; Prinzregentenstraße 159, 81677 München (DE).

(72) Erfinder: **SCHWARTZ, Udo**; Zugspitzstraße 8, 81541 München (DE). **STADLER, Kurt**; Am Forstanger 20, 82041 Oberhaching (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

(54) **Title:** IDENTIFYING AN IDENTITY CARRIER

(54) **Bezeichnung:** IDENTIFIZIEREN EINES IDENTITÄTSTRÄGERS

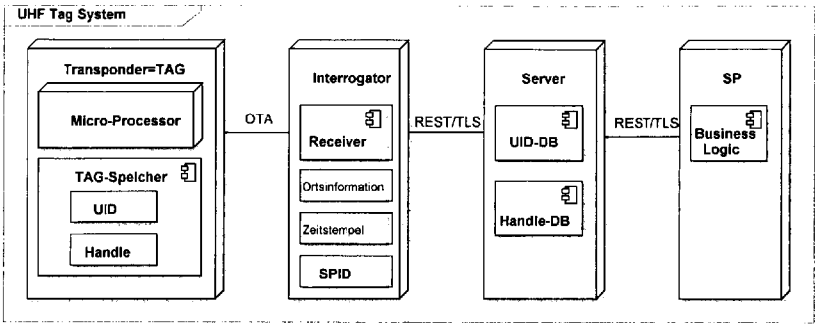

Fig. 1

(57) **Abstract:** The invention relates to a method for identifying an identity carrier (TAG) with an ID stored thereon, having the following steps: a) reading the ID from the identity carrier (TAG) using an interrogator; and b) transmitting the ID to a server using the interrogator, said server comprising a database with a plurality of IDs from a plurality of identity carriers, and identifying the identity carrier (TAG) using the read ID, wherein the method is characterized by the following features: the read ID is concealed using the following measures: the ID is now only read as a hash value calculated using a salt; for each ID with an assigned handle, the assigned handle is stored with the ID in the database; the handle is read as a fuzzy ID which is generated by applying a fuzzy algorithm with a specified hamming distance (t) to the handle; a fuzzy search is carried out in the server using the fuzzy ID, said fuzzy search providing a plurality of candidate handles; for each candidate handle, the assigned ID is ascertained; a comparison hash value is calculated for each candidate ID ascertained in this manner by applying the hash algorithm to the candidate ID and the transmitted salt in order to generate a plurality of comparison hash values; the comparison hash values are compared with the hash value transmitted to the server; and the identity carrier with the ID whose comparison hash value matches the hash value transmitted to the server is identified.

(57) **Zusammenfassung:** Die Erfindung schafft ein Verfahren zum Identifizieren eines Identitätsträgers (TAG) mit einer darin abgespeicherten ID, umfassend die Schritte: a) Auslesen der ID aus dem Identitätsträger (TAG) durch einen Interrogator; b) durch den Interrogator, Übertragen der ID an einen Server, der eine Datenbank mit einer Mehrzahl von IDs von einer Mehrzahl von Identitätsträgern umfasst, und Identifizieren des Identitätsträgers (TAG) anhand der ausgelesenen ID; und ist gekennzeichnet durch folgende Merkmale. Verschieiern der ausgelesenen ID durch folgende Maßnahmen. Die ID wird nur als mit einem Salt berechneter Hashwert ausgelesen.

WO 2017/178114 A9

[Fortsetzung auf der nächsten Seite]

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(48) Datum der Veröffentlichung dieser berichtigten Fassung:

07. Dezember 2017 (07.12.2017)

(15) Informationen zur Berichtigung:

siehe Mitteilung vom 07. Dezember 2017 (07.12.2017)

In der Datenbank des Servers ist zu jeder ID, der eine Handle zugeordnet ist, der zugeordneten Handle mit der ID abgespeichert. Die Handle wird als Fuzzy-ID ausgelesen, die durch Anwenden eines Fuzzy- Algorithmus mit einem vorbestimmten Hamming- Abstand (t) auf die Handle erzeugt ist. Beim Server wird mittels der Fuzzy-ID eine Fuzzy-Suche durchgeführt, die eine Mehrzahl von Kandidaten-Handies liefert. Zu jeder Kandidaten-Handle wird die zugeordnete ID ermittelt. Für die hierdurch festgelegten Kandidaten-IDs wird je ein Vergleichs-Hashwert berechnet, durch Anwenden des Hash- Algorithmus auf die Kandidaten-ID und den übertragenen Salt, um eine Mehrzahl von Vergleichs-Hashwerten zu erzeugen. Die Vergleichs-Hashwerte werden mit dem an den Server übertragenen Hashwert verglichen. Derjenige Identitätsträger, für dessen ID der Vergleichs-Hashwert mit dem an den Server übertragenen Hashwert übereinstimmt, ist identifiziert.

Identifizieren eines Identitätsträgers

Gebiet der Erfindung

Die Erfindung betrifft das Gebiet des Identifizierens eines Identitätsträgers mittels Auslesens von Identitätsdaten, im Zusammenhang mit der Erfindung auch einfach als ID bezeichnet, aus einem Identitätsträger durch einen Interrogator (Erfassungsgerät) über eine Kontaktlosschnittstelle (Funkschnittstelle, OTA-Schnittstelle).

Stand der Technik

In existierenden ID-Systemen wird eine ID aus einem Identitätsträger, z.B. einem RFID-Tag, an einen Interrogator, z.B. RFID-Lesegerät, übertragen und der Identitätsträger anhand der übertragenen ID identifiziert. Die Abfrage ist meist passiv, d.h. der Vorgang Bedarf keiner Aktion des Subjekts und damit auch keiner expliziten Zustimmung. Zudem erfolgt die Abfrage über eine Luftschnittstelle, und wird aktiviert, sobald sich der Identitätsträger innerhalb der Erfassungsdistanz des Interrogators befindet.

In Verbindung mit dem Interrogator steht ein Server, der ausgelesene IDs von einer Vielzahl von Interrogatoren entgegennimmt und auswertet.
In Verbindung mit dem Server steht ein Service-Provider. Dieser ist ein System, durch das ein computerimplementiertes Geschäftsmodell, nachfolgend als Business Logic bezeichnet, verwirklicht ist. Die Business Logic kann ein beliebiger Anwendungsfall eines ID-Systems sein, beispielsweise Logistik, Lagerhaltung, Zugriffsrechteverwaltung etc..

Das Senden der ID vom Identitätsträger kann passiv (automatisch, indem der Identitätsträger in den Erfassungsbereich des Interrogators kommt) oder aktiv (gesteuert durch den User) erfolgen. Die ID wird vom Interrogator aufgenommen und an den Server geleitet. Dort wird die ID ausgewertet.

Bei einem einfachen Ausleseverfahren wird die ID in Klartext aus dem Identitätsträger heraus an den Interrogator übertragen. Hierdurch ist mit dem Auslesen und anschließenden Auswerten am Server die Identifizierung bereits erreicht. Die Identifizierung ist somit sehr leicht und einfach zu erzielen. Die ID ist andererseits für jedermann mitlesbar. Zudem kann jedermann anhand der ausgelesenen ID den Aufenthaltsort des Identitätsträgers mitverfolgen (Tracking).

Die Mitlesbarkeit der ID stellt prinzipiell eine Verletzung der Privatsphäre dar, die unter Umständen unerwünscht ist. Auch die Mitverfolgbarkeit, also Trackbarkeit, der ID kann unerwünscht sein.

Eine direkte Lösung, um die Privatsphäre zu sichern, ist, die ID in verschlüsselter Form im Tag abzulegen. Bei einer solchen Lösung ist ein Schlüsselmanagement erforderlich, was Aufwand bedeutet. Wird ein Tag-individueller symmetrischer Schlüssel verwendet, muss dieser im Tag abgelegt sein, was ein Sicherheitsrisiko bedeutet. Wird ein Schlüsselableitungsverfahren verwendet, muss das Tag aufwändige kryptographische Berechnungen durchführen können. Tracking einzelner Tags ist auch bei verschlüsselt aus dem Tag ausgelesener ID immer noch möglich.

Ein gegen Tracking gesichertes Auslesen (Scan) von Identitäten mit elektronischen Verfahren insbesondere über die Luftschnittstelle (RFID, OTA) muss zwei zunächst widersprüchliche Ziele Erfüllen: Einerseits muss die Identität zuverlässig übertragen und an das System im Hintergrund gemeldet werden, andererseits soll es einem externen Angreifer nicht möglich sein, den Identitätsträger zu identifizieren und zu verfolgen.

Bei jeder Abfrage müssen Daten zwischen einem Identitätsträger und dem System, das die Identität feststellt (Interrogator) ausgetauscht werden. Tracking zu verhindern bedeutet, dass der Datenaustausch anonymisiert werden muss, sodass ein Angreifer, der Zugriff auf aus dem Identitätsträger ausgelesene Daten hat, weder die Identität selbst feststellen kann, noch Daten aus verschiedenen Abfrage-Vorgängen einer bestimmten Identität zuordnen kann.

Sicherheitsrelevant sind somit zusammenfassend zwei grundsätzliche Angriffe möglich: Zum einen wird die Privatsphäre des Subjekts beeinträchtigt, da ein Angreifer die Identität abfragen kann, ohne dass das Subjekt davon Kenntnis erhält oder seine Zustimmung geben muss. Zum zweiten kann ein Angreifer ein Subjekt über die Registrierung an verschiedenen Interrogatoren verfolgen (Tracking).

Aufgabe der Erfindung

Der Erfindung liegt die Aufgabe zu Grunde, ein Verfahren anzugeben, um Identitätsdaten (eine ID) aus einem Identitätsträger (z.B. RFID Tag, Mobiltelefon, Smartphone etc.) derart verschleiert an einen Interrogator zu übertragen, dass es dem Abfragesystem möglich ist, den Identitätsträger anhand der ausgelesenen Identitätsdaten zu identifizieren, und das gleichzeitig sicherstellt, dass ein externer Angreifer durch Inspektion der übertragenen oder in Übertragung befindlichen Identitätsdaten keinen Zugriff auf die Identität selbst erhält (Schutz der Privatsphäre) und Daten von verschiedenen Abfragen nicht eindeutig einer Identität zuordnen kann (Anti-Tracking).

Zusammenfassung der Erfindung

Die Aufgabe wird gelöst durch ein Verfahren zum Identifizieren eines Identitätsträgers mit einer darin abgespeicherten ID nach Anspruch 1.

Das Verfahren umfasst die Schritte: a) Auslesen der ID aus dem Identitätsträger durch einen Interrogator; b) durch den Interrogator, Übertragen der ID an einen Server, der eine Datenbank mit einer Mehrzahl von IDs von einer Mehrzahl von Identitätsträgern umfasst, und Identifizieren des Identitätsträgers anhand der ausgelesenen ID. Das Verfahren ist gekennzeichnet durch das Verschleiern der ausgelesenen ID. Das Verschleiern wird durch folgende Maßnahmen erreicht. Im Identitätsträger wird, zusätzlich zur ID, eine der ID eindeutig zugeordnete Handle gespeichert. In der Datenbank des Servers wird, zu jeder ID, der eine Handle zugeordnet ist, der zugeordnete Handle mit der ID abgespeichert, so dass in der Datenbank anhand einer Handle die zugeordnete ID auffindbar ist. Die Handle ist eine Zweit-ID, die es erlaubt, die direkte Verwendung der echten ID zu vermeiden. Weiter wird ein Hashwert durch Anwenden eines Hash-Algorithmus auf die ID und einen zufälligen Salt berechnet. Hierdurch ist die echte ID irreversibel anonymisiert und kann gefahrlos ausgelesen werden. Zudem wird eine Fuzzy-ID durch Anwenden eines Fuzzy-Algorithmus mit einem vorbestimmten Hamming-Abstand auf die Handle berechnet. Die Handle ist hierdurch verschleiert, behält aber genug rekonstruierbare Information über die echte Handle (nicht über die echte ID!), dass durch eine nachfolgende Fuzzy-Suche die echte Handle wieder aufgefunden werden kann.

Das Verfahren umfasst weiter:
den Schritt a) (Ausleseschritt), umfassend folgende Teilschritte:
- Auslesen der ID in Form des Hashwertes zusammen (= irreversibel anonymisierte ID) mit dem bei der Hashwert-Berechnung verwendeten Salt;
- Auslesen der berechneten Fuzzy-ID (= lediglich verschleierte Handle); und
den Schritt b) (Übertragungs- und Auswerteschritt), um über den Umweg der Handle schließlich die echte ID zu ermitteln, mit folgenden Teilschritten:
- um das Übertragen der ID zu bewirken, Übertragen des Hashwerts und

des Salt an den Server;
- beim Server, mittels der Fuzzy-ID (verschleierte Handle), Durchführen einer Fuzzy-Suche, und als Ergebnis der Fuzzy-Suche, Festlegen einer Mehrzahl von Kandidaten-Handles, die gemäß der Fuzzy-Suche zum Berechnen der Fuzzy-ID (verschleierten Handle) verwendet worden sein könnten;
- zu jeder ermittelten Kandidaten-Handle, ermitteln der zugeordneten ID (d.h. potentiellen echten ID), um eine entsprechende Mehrzahl von Kandidaten-IDs festzulegen;
- für jede festgelegte Kandidaten-ID, Berechnen eines Vergleichs-Hashwerts durch Anwenden desselben Hash-Algorithmus wie beim Berechnen des Hashwerts, auf die jeweilige Kandidaten-ID und den an den Server übertragenen Salt, um eine Mehrzahl von Vergleichs-Hashwerten zu erzeugen;
- Vergleichen der Mehrzahl von Vergleichs-Hashwerten mit dem an den Server übertragenen Hashwert;
- Identifizieren desjenigen Identitätsträgers, für dessen ID der Vergleichs-Hashwert mit dem an den Server übertragenen Hashwert übereinstimmt, als Identitätsträger, dessen ID - in Form des Hashwert - ausgelesen wurde.

Gemäß der Erfindung wird die ID in Klartext-Form selbst nicht in der Nachricht aufgenommen, sondern nur ein davon abgeleiteter Hash-Wert. Ferner wird für jede Übertragung ein Zufallswert generiert, der in den Hash eingeht und zusätzlich in die Nachricht aufgenommen wird.
Zusätzlich wird in der Nachricht eine Handle übertragen. Die Handle ist ein technischer Schlüssel, der die ID eindeutig adressiert. Die Handle ist im Device fest gespeichert. Bei der Übertragung wird die Handle mit einer zufälligen „Noise" Quelle verknüpft, sodass anstatt der Handle selbst eine Fuzzy ID mit einem fest definierten Hamming Abstand übertragen wird.
Die Nachricht wird über den Empfänger an den Server geleitet. Der Server wertet zunächst die Fuzzy-ID aus und führt einen Fuzzy Suche (Bereichs-

Suche oder Range Query) über eine Datenbank aus, die alle vergebenen Handles enthält. Da der Hamming-Abstand eine Metrik darstellt (die Dreiecks-Ungleichung ist erfüllt) können effiziente Fuzzy-Suchalgorithmen eingesetzt werden. Die Suche wird im Allgemeinen eine Anzahl von möglichen Handles ergeben.

Für jedes Suchergebnis wird nun die zugehörige ID ermittelt. Von der ID wird der Hash unter Verwendung des Salt aus der Nachricht gebildet und mit dem übertragenen Hash Wert verglichen. Unter der Voraussetzung dass der Hash kollisionsfrei ist wird in der zweiten Phase somit genau eine passende ID ermittelt, die dann die Grundlage für die weitere Verarbeitung ist.

Die Vorteile des Verfahrens sind:

- Es werden keine kryptologischen Verfahren verwendet; damit sind auch keine Schlüssel und keine Verfahren zur Schlüssel-Verteilung erforderlich.
- Die übertragene Nachricht ist für einen Angreifer nicht einer ID zuordenbar. Da nur der Hash Wert über die ID übertragen wird und die Hash-Funktion nicht umkehrbar ist (Trapdoor), kann aus dem Hash nicht auf die ID rückgeschlossen werden.
- Da ein zufälliger Salt verwendet wird, wird der Hash für die gleiche ID bei jedem Sendevorgang anders sein, sodass über den Hash auch kein Tracking erforderlich ist.
- Die Handle wird als Fuzzy-ID übertragen. Somit wird die Handle auch bei jeder Übertragung anders sein, sodass ein triviales Tracking auch über die Handle nicht möglich ist.
- Alle Handles einer ID haben jedoch einen definierten Hamming Abstand zueinander. Dies könnte ein Angreifer ausnutzen, um Tracking zu erreichen. Das Verfahren geht jedoch davon aus, dass der Hamming Abstand so groß gewählt wird, dass immer eine ausreichende

Anzahl von IDs durch die Handle plus den Hamming Bereich möglich sind. Der Angreifer, der keine Kenntnis über die Menge der vergebenen Handles hat, wird somit nur eine ständig variierende Gruppe von IDs tracken können.

- Umgekehrt kann der Server ausgehend von der Kenntnis der vergebenen Handles immer effizient alle passenden Handles zu einer Fuzzy-ID ermitteln.
- Durch die Größe des Wertebereichs der Handle und den Hamming Abstand kann die Tracking Granularität eingestellt werden. Damit sind feine Abstimmungen zwischen Tracking-Granularität und Performance möglich.

Wahlweise umfasst der Salt eine durch den Identifikator erzeugte Zufallszahl. Wahlweise – alternativ oder zusätzlich zur vom Identifikator erzeugten Zufallszahl, umfasst der Salt eine durch den Interrogator erzeugte Nonce, insbesondere (ebenfalls) eine Zufallszahl, die vor Berechnen des Hashwerts durch den Interrogator an den Identitätsträger gesendet wird.

Der Hamming-Abstand des Fuzzy-Algorithmus wird wahlweise so festgelegt, dass bei der Fuzzy-Suche mindestens eine vorbestimmte Mindestzahl von Kandidaten-Handles festgelegt wird, um eine gewisse Verschleierung der wahren Handle zu erreichen. Andererseits darf die Anzahl der Kandidaten-Handles nicht zu hoch sein. Steigt die Anzahl Kandidaten-Handles, gibt es auch zunehmend Kandidaten-Handles, die auf mehrere unterschiedliche echte IDs zurückführen. Ein Rückschluss von einem Kandidaten-Handle auf eine eindeutige ID kann somit zunehmend erschwert oder sogar unmöglich werden. Die Mindestzahl Kandidaten-Handles soll mindestens zehn sein, kann aber auch bis auf mehrere tausend gesteigert werden, mit einer optima-

len Kandidaten-Anzahl abhängig von diversen Parametern im System, z.B. in Bereich von 10 bis 10000 oder, enger von 50 bis 500 Kandidaten-Handles.

Kurzbeschreibung der Figuren

Ausführungsbeispiele werden anhand der Figuren dargelegt, worin zeigen:

Fig. 1 ein Abfragesystem gemäß einer Ausführungsform der Erfindung;

Fig. 2 einen Scan (TAG-Auslesevorgang) im Abfragesystem aus Fig. 1;

Fig. 3 eine Tabelle mit dem zu wählenden Hamming-Abstand t, um die Anzahl von Überschneidungen s bei gegebener Anzahl von Handles und der Handle-Bitlänge n zu erreichen.

Detaillierte Beschreibung

Fig. 1 zeigt ein Abfragesystem gemäß einer Ausführungsform der Erfindung, wobei als Identitätsträger ein Transponder oder, gleichbedeutend, TAG vorgesehen ist, also ein Funketikett mit Chip und Antenne, z.B. ein RFID-Tag oder UHF-Tag. Die Lösung wird realisiert durch das Zusammenwirken der folgenden in Fig. 1 dargestellten Komponenten.

Transponder= TAG: Der Transponder ist im Besitz des ID-Trägers (endusers). Eine mögliche Ausführungsform ist ein RFID-Tag. Der Transponder kann mittels seiner Antenne Nachrichten über die Luftschnittstelle an den Interrogator senden und auch Nachrichten vom Interrogator empfangen (bidirektionale Kommunikation). Der Transponder-Chip in der erfindungsgemäßen Ausführung umfasst einen Prozessor, nämlich den Micro-Prozessor, und einen Speicher, nämlich den Tag-Storage.

Micro-Processor: Der Prozessor auf dem Transponder kann Daten vom Speicher sowie aus Nachrichten verarbeiten. Der Prozessor wird entweder durch eine Stromquelle auf dem Transponder selbst (aktiv) oder durch die Energie aus der Nachrichten-Übertragung (z.B. Funksignal) betrieben.

Tag-Storage: Im Tag-Storage (Tag-Speicher) sind die ID des Transponders, hier als UID bezeichnet, und eine Handle gespeichert. Das TAG-Storage kann Daten persistent speichern. In der hier zugrunde liegenden Ausführung ist nur lesender Zugriff verlangt. Es wird davon ausgegangen, dass die Daten UID und Handle einmalig in einem Provisionierungsschritt auf das TAG aufgebracht werden. Die Daten stehen dem Micro-Processor des TAG lesend zur Verfügung.

Interrogator: Der Interrogator ist ein Transponder-Lesegerät. Er initiiert die TAG Interaktion. Ziel des Interrogators ist es, am TAG einen Scan, d.h. einen Auslesevorgang durchzuführen, bei dem ID und Handle in verfälschter Form ausgelesen werden. Der Interrogator kann über die Luftschnittstelle (OTA) mit dem Transponder kommunizieren. Der Interrogator kann sowohl Nachrichten an den Transponder senden als auch Nachrichten vom Transponder empfangen. Der kann weiter Daten an den Server senden. Nachdem der Interrogator ein TAG ausgelesen hat und die Daten des TAG in einer Nachricht empfangen hat, erweitert der Interrogator die Nachricht mit seine spezifischen Interrogator-Attributen und sendet die erweiterte Nachricht an einen Server in einer „ScanEvent"-Nachricht.

Server: Der Server hat eine Datenbank, in der zu einer Vielzahl von Transpondern Paare von zusammengehörigen IDs und Handles gespeichert sind. Empfängt der Server von einem Interrogator eine Nachricht, ist es sein Ziel, zu ermitteln, zu welchem Transponder die Nachricht gehört. Die Handles können sich in Lauf der Zeit ändern. Ist dies der Fall, muss die Datenbank jeweils aktualisiert werden. Der Server empfängt die ScanEvent-Notifikation zum Scan-Ereignis und ermittelt in der unten beschriebenen Weise die UID. Danach signalisiert er das Scan-Ereignis mit einer „Event"-Nachricht an den zugeordneten Service Provider SP.

SP: Der SP (Service Provider) ist ein Server der vom Dienst-Anbieter betrieben wird. Es ist die Aufgabe dieses Servers die dem Scan-Ereignis entsprechenden Aktion auf der Ebene des Business Prozesses auszuführen.
UID: Die ID eines Transponders (TAGs) ist eine festgelegte und im Allgemeinen unveränderbare Zahl.
Handle: Die Handle ist eine frei wählbare Zweit-Identität des Transponders, die um Unterschied zur festgelegten eigentlichen ID also insbesondere bei Bedarf immer wieder neu festgelegt werden kann, z.B. als bei Bedarf immer wieder neu generierte Zufallszahl. Nur eine Teilmenge aller möglichen Handles ist tatsächlich für Transponder vergeben. Durch die Teilmenge der tatsächlich vergebenen Handles in Relation zur Gesamtmenge der konstruktiv möglichen Handles ist der später noch verwendete Füllgrad definiert.

Teilweise sind in den Figuren an das Englische angelehnte Kommandos angegeben, die als nicht übersetzbar angesehen werden. Insbesondere werden folgende Kommandos verwendet.
Select(): vom Interrogator an das TAG gesendet, um einen Scan, zu starten.
SHA(): Hashwert-Berechnung.
FuzzyID(): Berechnung einer Fuzzy-ID FUZZY.
Reply(): Antwortnachricht vom TAG an den Interrogator.
ScanEvent(): Kommando, mit dem der Interrogator den Server über das Ereignis eines Auslesens des TAGs informiert und Daten, die der Interrogator aus dem TAG ausgelesen hat, an den Server weiterleitet, ggf. zusammen mit weiteren Daten, die der Interrogator hinzufügt.
Lookup(): Kommando, mit dem der Server bei sich selbst eine Suchabfrage durchführt, um einen Eintrag in der Datenbank zu finden.
Event(): Kommando, mit dem der Server den Service Provider über ein aufgetretenes Ereignis informiert.

RangeQuery(): Fuzzy-Suche in der ID/Handle-Datenbank des Servers, bei der nach einem Bereich („Range") von mehreren Einträgen gesucht wird.

Fig. 2 zeigt einen Scan, d.h. Abfragedurchlauf im Abfragesystem aus Fig. 1.

Der Ablauf des Scan umfasst die folgenden Schritte1.0-2.5.

1.0 Generate(): nonce [Nonce-Erzeugung = optionaler Schritt]

Der Interrogator erzeugt eine Nonce. Die Generierung kann auf Basis eines Zufallszahlengenerators erfolgen

1.1 Select(nonce) [oder Select()]

Der Interrogator sendet ein Select Signal an den Transponder. Mit dem Select Signal wird der Scan (Abfragedurchlauf) eingeleitet. Falls vom Interrogator eine Nonce erzeugt wurde, wird die Nonce mit dem Select() Signal mit übersendet und an den Transponder übergeben.

1.2 SHA(salt, UID): SHA [oder SHA(salt,nonce,UID) oder SHA(nonce,UID)]

Der Transponder berechnet über die UID und einen Salt einen Hashwert. Der Salt wird wahlweise auf dem Transponder generiert (z.B. durch einen Zufallszahlengenerator). Alternativ wird die vom Interrogator empfangene Nonce direkt als Salt verwendet. Alternativ werden als Salt ein vom Transponder generierter eigener Salt und die vom Interrogator an den Transponder übertragene Nonce zusammen als Salt verwendet.

1.3 Fuzzy(Handle, h): FUZZY

Der Transponder erzeugt eine Fuzzy-ID FUZZY aus der Handle. Dazu werden maximal h zufällige Bits der Handle invertiert.

2.0 Reply(salt, SHA, FUZZY)

Der Transponder sendet den Salt, den Hash-Code SHA und die Fuzzy-ID FUZZY an den Interrogator.

2.1 ScanEvent(location, datetime, SPID, salt, SHA, FUZZY)

Der Interrogator teilt mit einer „ScanEvent()" Nachricht an den Server das TAG-Auslese-Ereignis mit. Der Interrogator ist mit spezifischen Attributen

konfiguriert (z.B. einer Ortsinformation „location" des Interrogators, und einer Service Provider-Identität SPID eines Service-Providers, der den Interrogator betreibt). Ferner ermittelt der Interrogator einen Zeitstempel „Datetime". Der Interrogator vervollständigt die vom TAG erhaltene Nachricht mit Interrogator-spezifischen Attributen und dem Zeitstempel. Der Interrogator gibt die vom Transponder empfangenen Daten weiter an den Server.

2.2 RangeQuery(FUZZY, h): List<handle>

Der Server führt eine "Range"-Query über die Handle-Datenbank aus. Eine Range-Query sucht nicht nur nach einem einzelnen Record, d.h. Eintrag, in einer Datenbank, sondern ermittelt alle Records, die in einem Intervall um einen Suchwert liegen. Das Ergebnis der RangeQuery Abfrage ist eine Mehrzahl von Handles, die in dem abgefragten Intervall liegen.

2.3 Lookup(handle): UID

Für jede Handle der Mehrzahl von Handles aus der Range-Query ermittelt der Server die zugehörige UID. Dies ist möglich da eine eindeutige Zuordnung zwischen Handle und UID besteht.

2.4 SHA(salt, UID): hash

Der Server berechnet für jede UID aus der Range-Query den Hash-Wert nach, wie ihn der Transponder selbst berechnet hat, unter Benutzung des Salt aus der Notifikation vom Interrogator. Wenn der so errechnete Hash-Wert gleich dem Hash-Wert aus der Nachricht ist, ist die richtige UID gefunden.

2.5 Event(location, datetime, SPID, UID)

Der Server sendet eine Nachricht an den SP-Server und meldet das Scan Event. Der SP kann nun die Information über die identifizierte ID in der Business Logic anwenden.

Die Range-Query hat als Suchwert die Fuzzy-ID FUZZY. Die Länge des Such-Intervalls ist der maximale Hamming-Abstand h (der max Hamming Abstand ist eine systemweite Konstante). Da der Hamming Abstand eine

Metrik ist (die Dreiecksungleichung ist erfüllt) sind die Voraussetzung für eine effiziente Range-Query erfüllt. Der Server kann die IDs in logarithmischer Zeit ermitteln.

Die Handle ist eingeführt, obwohl eine eins-zu-eins Beziehung zwischen der Handle und der UID besteht. Die UID kann nicht direkt verwendet werden, da die UID nie in den übertragenen Daten erscheinen soll. Zudem soll auch eine optimale Verteilung der Werte für die Range-Query erreicht werden. Außerdem soll erreicht werden, dass immer ausreichend viele Werte im Hamming Abstand zu jeder Handle liegen. Dies ist in der Regel nur durch einen durch das System vergebenen Wert für die Handle sichergestellt.

Zusammenfassend werden vom Interrogator zum Transponder folgenden Daten übertragen:

- Nonce (zufälliger Wert)

Vom Transponder zum Interrogator werden die folgenden Daten gesendet:

- Salt (zufällig gewählter Wert)
- Hash über UID (mit Salt)
- Fuzzy-Handle (von tatsächlicher Handle abgeleitet, mit max h bits umgeschaltet)

Die angestrebte Absicherung gegen einen Tracking-Angriff erfordert eine sorgfältige und abgestimmte Auswahl des Wertebereichs des Handle und des maximalen Hamming Abstandes t.

Im Folgenden gehen wir von einem binären Alphabet $A = \{0, 1\}$ aus. Handles x oder y sind dann Blockcodes mit der Bitlänge n und bilden in ihrer Gesamtheit eine Menge: $C \subseteq A^n$ möglicher Handles x, y.

Eine Kugel K vom Radius t bezogen auf den Hamming Abstand d und einen bestimmten Handle x sei definiert wie folgt:

$$K_t(x) = \{ y \in C : d(x,y) \leq t \}$$

Dabei soll d(x, y) den Hamming Abstand zweier Handles x, y zueinander bezeichnen und t den für die Kugel K maximal zulässigen Hamming Abstand t.

$K_t(x)$ ist eine Teilmenge von A^n. Die Mächtigkeit von $K_t(x)$ errechnet sich wie folgt:

$$N_t = \sum_{k=0}^{t} \binom{n}{k}$$

Der maximale Hamming Abstand t und der Wertebereich der Handles x (bzw. y), die in dieser Kugel K liegen, soll so gewählt werden, dass es für jedes beliebige $x \in C$ eine Menge $Y \subseteq C$ gibt mit der folgenden Eigenschaft:

$$\forall y \in Y : K_t(x) \cap K_t(y) \neq \emptyset$$

Das heißt mit anderen Worten, die Anzahl der Handles x, y muss größer als die Kugelpackungsschranke (Hamming-Schranke) $|C|$ sein. Die Kugelpackungsschranke $|C|$ bei gegebener Bitlänge n und maximalem Hamming-Abstand t berechnet sich wie folgt:

$$|C| = \frac{2^n}{\sum_{i=0}^{t} \binom{n}{j}}$$

Wenn die Anzahl der Handles x, y unterhalb der Kugelpackungsschranke $|C|$ liegt, kann der Angreifer eine mitgehörte Handle dekodieren und einem originalen Handle zuordnen, wenn er Kenntnis aller Handles hätte (was in der Praxis allerdings nicht der Fall ist).

Die Unsicherheit für den Dekodierer (den Angreifer) erhöht sich, je mehr Blockcodewörter (Handles) x definiert sind, je größer der maximale Hamming Abstand t ist und je kleiner die Bitlänge n gewählt wird.

Die Tabelle in Fig. 3 stellt eine Abschätzung dieses Zusammenhangs dar.

Als Grundlage für das Maß für die Unsicherheit des Dekodierers (Angreifers) ist die Überschneidungsmenge S von Kugeln K für Handles c ∈C in Bezug auf eine Kugel K(x) um ein spezielles Handle x angenommen, die wie folgt definiert ist:

$$S_t(x) = \{c \in C : K_t(c) \cap K_t(x) \neq \emptyset\}$$

Als eigentliches Maß für Unsicherheit selbst bzw. die Güte der Privacy-Protection soll die minimale Mächtigkeit von S für alle gültigen Code-Wörter / Handles c angenommen werden:

$$s_t = \min_{c \in C} |S_t(c)|$$

Die Tabelle in Fig. 3 zeigt in den Tabellenfeldern im rechten Teil der Tabelle die maximale Hamming-Distanz t, die gewählt werden müsste, um eine vorgegebene Überschneidung (Unsicherheit s) zu erreichen. In Analogie zur Berechnung der Kugelpackungsschranke |C| wird für die Berechnung die Überbelegung des verfügbaren Code-Raums durch die Kugeln K herangezogen. Die Tabelle Fig. 3 ist wie folgt zu lesen:

- Die Kopfzeile im rechten Teil der Tabelle gibt die geforderte Überschneidung s bzw. die Unsicherheit an, mit exemplarischen Überschneidungs-Werten s = 1, 5, 10, 20, 100, 500, 1000 und 2000
- Die erste Spalte zeigt die Länge n des Blockcodes (Bit-Länge), d.h. des Handles x, mit Bit-Länge-Werten n = 8, 16, 24, 32, 48 und 64
- Die zweite Spalte zeigt die Anzahl |C| der gültigen Code-Wörter; dies entspricht der Anzahl |C| der verwendeten Handles
- Die dritte Spalte zeigt den Füllgrad f (Fill %) und damit die definierten Handles als relative Größe in Bezug auf die Gesamtzahl der möglichen Block-Codes (die Formel liefert Werte im Bereich 0..1, die Tabelle zeigt die entsprechenden Prozentwerte):

$$f = \frac{|C|}{2^n}$$

Der Füllgrad f ist somit das Verhältnis zwischen den möglichen Handles im Code-Raum zu den tatsächlich definierten Handles. Zum Beispiel, bei einer Bitlänge n von 8 Bit und 25 definierten Handles ist der Füllgrad f ca. 10%.

- Die restlichen Spalten zeigen den Hamming-Abstand t, der gewählt werden müsste, um die in der Kopfzeile gegebene Unsicherheit s = 1, 5, 10, ... bzw. 2000 zu erreichen

Grundlage für die Werte in der Tabelle ist die folgende Berechnung der Überbelegung tab (n,c,s) des verfügbaren Code-Raums durch die Menge aller Kugeln K_t:

$$tab(n,c,s) = \min_t \left(\frac{N_t * c}{2^n} \geq s \right)$$

Mit anderen Worten: Eine Kugel K_t gibt die für eine Handle mögliche Menge von Block-Codes C mit dem gewählten Hamming Abstand t an. Wenn die Summe der Mächtigkeit aller K_t für alle definierten Handles den Code-Bereich (2^n) um das s-fache übersteigt, ist dies eine hinreichende Bedingung für mindestens s Überschneidungen für jede definierte Handle, d.h.

$$\bigwedge_{x,y \in C} |K_t(x) \cap K_t(y)| \geq s$$

Die Parameter n,c ergeben sich aus der Zeile (wie in Spalte 1 und 2 angeben), der Parameter s ergibt sich aus der jeweiligen Spalte (siehe Kopfzeile). Die Werte in der Tabelle (Zellen) sind der nach der obigen Formel ermittelte minimale Hamming Abstand t.

Die Sektion mit der Bitlänge 8 hat nur informativen Charakter, aber keine praktische Bedeutung.

Für das Verfahren günstig ist ein ausreichend hoher Hamming-Abstand t und eine dünn besetzte Code-Space (|C| ist klein).

Da die Handles C technische Identifier sind, die durch das System generiert werden, kann durch den Generierungsalgorithmus sichergestellt werden,

dass es für fast alle Handles eine ausreichende Mehrdeutigkeit besteht, indem neue Handles solange wie möglich aus den Kugeln K_t bestehender Handles gewählt werden.

Der Nachweis des Schutzes der Identität ID ist trivial, er ist dadurch gegeben, dass nie die Identität selbst, sondern nur der Hash Wert übertragen wird. Ein Angreifer müsste die Hash-Funktion umkehren, um die tatsächliche Identität zu ermitteln. Eine geeignete Hash-Funktion vorausgesetzt gehen wir davon aus, dass dies nicht effizient möglich ist. Zudem würde ein erfolgreicher Angriff auf die Hash-Funktion nur eine einzige ID kompromittieren, das System selbst bliebe aber sicher.

Gegen Tracking schützt das erfindungsgemäße Verfahren wie folgt:
Der Hash-Wert ist mit einem zufälligen „Salt" geschützt. Das bedeutet, dass für jede Abfrage ein neuer Zufallswert „Salt" gebildet und in die Hash-Berechnung einbezogen wird. Der „Salt" ist in den Abfragedaten enthalten. Somit enthalten die Daten von verschiedenen Abfragen unterschiedliche Hash Werte (bis auf den Fall dass tatsächlich der gleiche Salt verwendet wird, was als sehr unwahrscheinlich angesehen werden kann).
Ein Tracking Angriff kann auch über die Handle geführt werden. Die Handle wird aber als Fuzzy-ID übertragen. Das bedeutet, auch die Handle wird in den Daten von verschiedenen Abfragen unterschiedlich sein.
Der Angreifer kann zwar den Hamming Abstand von zwei unterschiedlichen Fuzzy-Handles berechnen. Damit kann der Angreifer aber nur sicher feststellen, dass zwei Handles zu verschiedenen Identitäten gehören (weil der Hamming Abstand zu groß ist).
Zwei Handles $x, y \in A^n$, die nahe beieinander liegen (geringe Hamming-Distanz $d(x, y)$), können immer zu unterschiedlichen Identitäten gehören. Zum einen sollte der Hamming Abstand so gewählt werden, dass immer

Überschneidungen möglich sind, die aber der Server wegen der Kenntnis der vergebenen Handles leicht auflösen kann.

Zum anderen ist der Angreifer im Nachteil, da er nur die Fuzzy-Handles aber nicht den tatsächlichen Handle-Wert kennt. Letztlich bedeutet dies dass der Angreifer mit dem doppelten Hamming Abstand rechnen muss (wegen Kugel-Überschneidung):

Dies kann an dem folgenden Beispiel gezeigt werden (Annahme ist 8 Bit Handle-Länge n, und Hamming-Abstand t = 3):

Tatsächliches Handle:

1	0	1	0	1	0	1	0

Fuzzy-Handle, offen für Angreifer:

0	1	0	0	1	0	1	0

Mögliches Handle, mit Hamming Abstand t = 3 vom Fuzzy-Handle und Hamming Abstand t = 6 zum tatsächlichen Handle:

0	1	0	0	1	1	0	1

Als Spezialfall sei angemerkt, dass selbst zwei gleiche von einem Angreifer beobachtete Fuzzy-Handle-Werte somit zu unterschiedlichen Identitäten gehören können.

Patentansprüche

1. Verfahren zum Identifizieren eines Identitätsträgers (TAG) mit einer darin abgespeicherten ID, umfassend die Schritte:

a) Auslesen der ID aus dem Identitätsträger (TAG) durch einen Interrogator;

b) durch den Interrogator, Übertragen der ID an einen Server, der eine Datenbank mit einer Mehrzahl von IDs von einer Mehrzahl von Identitätsträgern umfasst, und Identifizieren des Identitätsträgers (TAG) anhand der ausgelesenen ID;

gekennzeichnet durch die Merkmale:

Verschleiern der ausgelesenen ID durch folgende Maßnahmen:

- im Identitätsträger (TAG), Gespeicherthalten oder Abspeichern einer der ID eindeutig zugeordneten Handle;
- in der Datenbank des Servers, zu jeder ID, der eine Handle zugeordnet ist, Abspeichern der zugeordneten Handle mit der ID, so dass in der Datenbank anhand einer Handle die zugeordnete ID auffindbar ist;
- Berechnen eines Hashwertes durch Anwenden eines Hash-Algorithmus auf die ID und einen zufälligen Salt;
- Berechnen einer Fuzzy-ID durch Anwenden eines Fuzzy-Algorithmus mit einem vorbestimmten Hamming-Abstand (t) auf die Handle;

und durch das Merkmal, dass

Schritt a) umfasst:

- Auslesen der ID in Form des Hashwertes zusammen mit dem bei der Hashwert-Berechnung verwendeten Salt;
- Auslesen der berechneten Fuzzy-ID; und

Schritt b) umfasst:

- um das Übertragen der ID zu bewirken, Übertragen des Hashwerts und des Salt an den Server;
- beim Server, mittels der Fuzzy-ID, Durchführen einer Fuzzy-Suche, und als Ergebnis der Fuzzy-Suche, Festlegen einer Mehrzahl von Kandidaten-Handles, die gemäß der Fuzzy-Suche zum Berechnen der Fuzzy-ID verwen-

det worden sein könnten;
- zu jeder ermittelten Kandidaten-Handle, ermitteln der zugeordneten ID, um eine entsprechende Mehrzahl von Kandidaten-IDs festzulegen;
- für jede festgelegte Kandidaten-ID, Berechnen eines Vergleichs-Hashwerts durch Anwenden desselben Hash-Algorithmus wie beim Berechnen des Hashwerts, auf die jeweilige Kandidaten-ID und den an den Server übertragenen Salt, um eine Mehrzahl von Vergleichs-Hashwerten zu erzeugen;
- Vergleichen der Mehrzahl von Vergleichs-Hashwerten mit dem an den Server übertragenen Hashwert;
- Identifizieren desjenigen Identitätsträgers, für dessen ID der Vergleichs-Hashwert mit dem an den Server übertragenen Hashwert übereinstimmt.

2. Verfahren nach Anspruch 1, wobei der Salt eine durch den Identifikator erzeugte Zufallszahl umfasst.

3. Verfahren nach Anspruch 1 oder 2, wobei der Salt eine durch den Interrogator erzeugte Nonce, insbesondere eine Zufallszahl, umfasst, die vor Berechnen des Hashwerts durch den Interrogator an den Identitätsträger (TAG) gesendet wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei der Hamming-Abstand (t) des Fuzzy-Algorithmus so festgelegt wird, dass bei der Fuzzy-Suche mindestens eine vorbestimmte Mindestzahl von Kandidaten-Handles festgelegt wird.

5. Verfahren nach Anspruch 4, wobei die Mindestzahl von Kandidaten-Handles im Bereich von zehn bis mehrere tausend liegt, weiter vorzugsweise im Bereich 10 bis 10000, weiter vorzugsweise im Bereich von 50 bis 500.

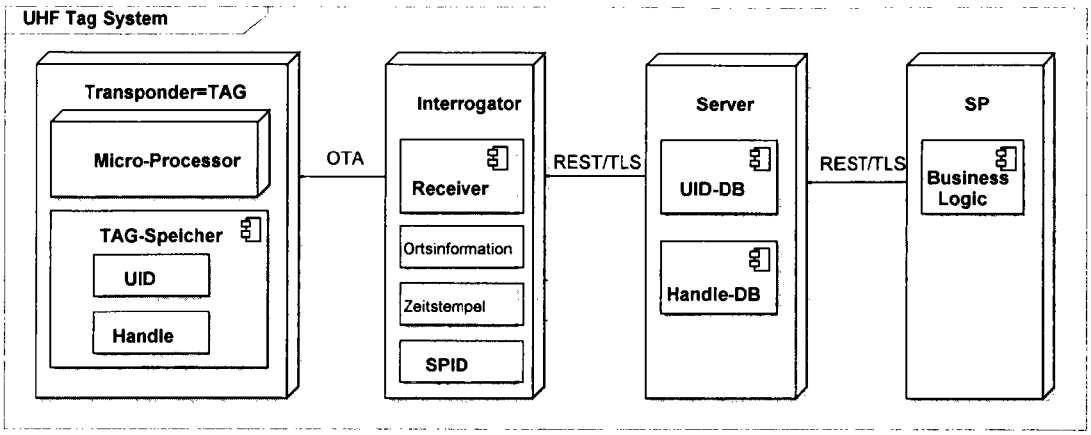
UHF Tag System
Transponder=TAG
Micro-Processor
TAG-Speicher
UID
Handle
OTA
Interrogator
Receiver
Ortsinformation
Zeitstempel
SPID
REST/TLS
Server
UID-DB
Handle-DB
REST/TLS
SP
Business Logic

Fig. 1

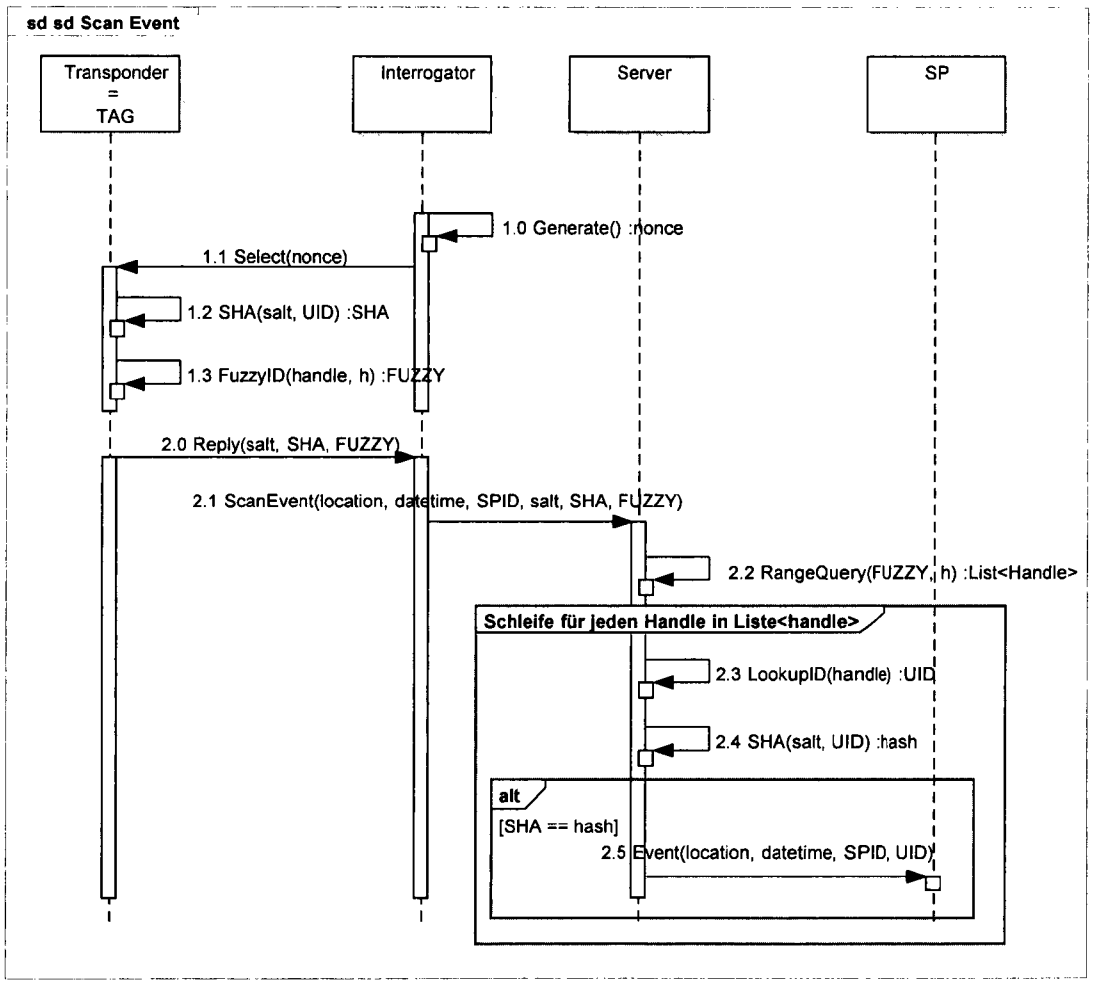
sd sd Scan Event
Transponder = TAG
Interrogator
Server
SP
1.0 Generate() :nonce
1.1 Select(nonce)
1.2 SHA(salt, UID) :SHA
1.3 FuzzyID(handle, h) :FUZZY
2.0 Reply(salt, SHA, FUZZY)
2.1 ScanEvent(location, datetime, SPID, salt, SHA, FUZZY)
2.2 RangeQuery(FUZZY, h) :List<Handle>
Schleife für jeden Handle in Liste<handle>
2.3 LookupID(handle) :UID
2.4 SHA(salt, UID) :hash
alt
[SHA == hash]
2.5 Event(location, datetime, SPID, UID)

Fig. 2

			s								
n	|C|	Fill %	1	5	10	20	100	500	1000	2000	
8	2	1,00%	4								
8	5	2,00%	3								
8	12	5,00%	2	4	5						
8	25	10,00%	2	3	4	5					
8	76	30,00%	1	2	2	3					
8	128	50,00%	1	2	2	3	5				
8	179	70,00%	1	1	2	2	4				
8	230	90,00%	1	1	2	2	4				
16	6	0,01%	6	10							
16	65	0,10%	4	5	6	7					
16	327	0,50%	3	4	4	5	7				
16	655	1,00%	2	3	4	4	6	9			
16	3.276	5,00%	2	2	3	3	4	6	7	9	
16	6.553	10,00%	1	2	2	3	4	5	6	7	
16	13.107	20,00%	1	2	2	2	3	4	5	6	
16	19.660	30,00%	1	2	2	2	3	4	5	5	
16	32.768	50,00%	1	1	2	2	3	4	4	5	
16	45.875	70,00%	1	1	1	2	3	4	4	5	
16	58.982	90,00%	1	1	1	2	2	3	4	4	
24	1.677	0,01%	4	5	6	7	8	11	13		
24	16.777	0,10%	3	4	4	5	6	7	8	9	
24	83.886	0,50%	2	3	3	4	5	6	7	7	
24	167.772	1,00%	2	3	3	3	4	5	6	7	
24	838.860	5,00%	1	2	2	3	3	4	5	5	t
24	1.677.721	10,00%	1	2	2	2	3	4	4	5	
24	3.355.443	20,00%	1	2	2	2	3	4	4	4	
24	8.388.608	50,00%	1	1	1	2	2	3	3	4	
24	11.744.051	70,00%	1	1	1	2	2	3	3	4	
24	15.099.494	90,00%	1	1	1	1	2	3	3	3	
32	429.496	0,01%	4	5	5	5	6	8	8	9	
32	4.294.967	0,10%	3	3	4	4	5	6	6	7	
32	42.949.672	1,00%	2	2	3	3	4	5	5	5	
32	429.496.729	10,00%	1	2	2	2	3	3	4	4	
32	858.993.459	20,00%	1	1	2	2	2	3	3	4	
32	2.147.483.648	50,00%	1	1	1	2	2	3	3	3	
32	3.865.470.566	90,00%	1	1	1	1	2	3	3	3	
48	28.147.497.671	0,01%	3	4	4	4	5	6	6	7	
48	281.474.976.710	0,10%	2	3	3	4	4	5	5	6	
48	1.407.374.883.553	0,50%	2	2	3	3	4	4	4	5	
48	2.814.749.767.106	1,00%	2	2	2	3	3	4	4	4	
48	14.073.748.835.532	5,00%	1	2	2	2	3	3	4	4	
48	140.737.488.355.328	50,00%	1	1	1	1	2	2	3	3	
64	1.844.674.407.370.950	0,01%	3	3	4	4	4	5	5	6	
64	18.446.744.073.709.500	0,10%	2	3	3	3	4	4	4	5	
64	92.233.720.368.547.700	0,50%	2	2	2	2	3	4	4	4	
64	184.467.440.737.095.000	1,00%	1	2	2	2	3	3	4	4	
64	3.689.348.814.741.910.000	20,00%	1	1	1	1	2	2	3	3	

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/000474

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04W12/06 H04L29/06 H04W4/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/045442 A1 (LU LI [HK] ET AL) 25 February 2010 (2010-02-25) paragraph [0055] - paragraph [0071]; figures 5,6,9 paragraph [0079] paragraph [0082] -----	1-5
A	US 2010/161999 A1 (POOVENDRAN RADHA [US] ET AL) 24 June 2010 (2010-06-24) paragraph [0013] paragraph [0101] - paragraph [0103] paragraph [0113] - paragraph [0116] paragraph [0125] - paragraph [0129] paragraph [0135] -----	1-5
A	US 2007/133807 A1 (LEE HANG R [KR] ET AL) 14 June 2007 (2007-06-14) paragraph [0035] - paragraph [0047] -----	1-5

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2017	07/07/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tenbieg, Christoph

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/000474

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010045442 A1	25-02-2010	NONE	
US 2010161999 A1	24-06-2010	US 2010161999 A1	24-06-2010
		US 2013207780 A1	15-08-2013
US 2007133807 A1	14-06-2007	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/000474

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04W12/02 H04W12/06 H04L29/06 H04W4/00
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04W H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2010/045442 A1 (LU LI [HK] ET AL) 25. Februar 2010 (2010-02-25) Absatz [0055] - Absatz [0071]; Abbildungen 5,6,9 Absatz [0079] Absatz [0082]	1-5
A	US 2010/161999 A1 (POOVENDRAN RADHA [US] ET AL) 24. Juni 2010 (2010-06-24) Absatz [0013] Absatz [0101] - Absatz [0103] Absatz [0113] - Absatz [0116] Absatz [0125] - Absatz [0129] Absatz [0135]	1-5
A	US 2007/133807 A1 (LEE HANG R [KR] ET AL) 14. Juni 2007 (2007-06-14) Absatz [0035] - Absatz [0047]	1-5

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. Juni 2017	07/07/2017

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tenbieg, Christoph

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/000474

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2010045442 A1	25-02-2010	KEINE	
US 2010161999 A1	24-06-2010	US 2010161999 A1	24-06-2010
		US 2013207780 A1	15-08-2013
US 2007133807 A1	14-06-2007	KEINE	