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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. November 2013 (28.11.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/174540 A1

(51) Internationale Patentklassifikation:
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/055923

(22) Internationales Anmeldedatum:
21. März 2013 (21.03.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 208 834.2 25. Mai 2012 (25.05.2012) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FALK, Rainer**; Primelweg 9, 85586 Poing (DE). **FRIES, Steffen**; Eberweg 3, 85598 Baldham (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

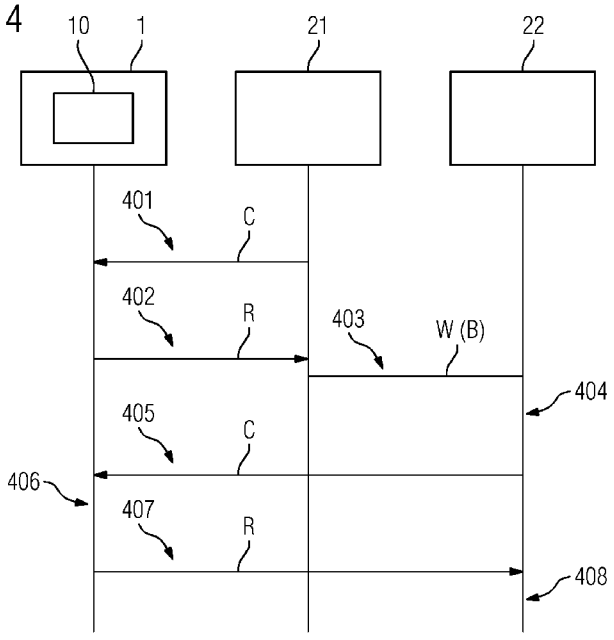
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

(54) **Title**: FUNCTION FOR THE CHALLENGE DERIVATION FOR PROTECTING COMPONENTS IN A CHALLENGE RESPONSE AUTHENTICATION PROTOCOL

(54) **Bezeichnung** : FUNKTION ZUR CHALLENGE-ABLEITUNG ZUM SCHUTZ VON KOMPONENTEN IN EINEM CHALLENGE-RESPONSE AUTHENTIFIZIERUNGSPROTOKOLL

FIG 4



(57) **Abstract**: The invention relates to a device for authenticating a product with respect to at least one authenticator. Said device comprises a capturing unit, a test unit and a transmitting unit. Said capturing unit is designed to capture a challenge emitted by the authenticator. Said test unit is designed to test an authorization from the authenticator for capturing a response to the emitted challenge. Said transmitter unit is designed to transmit a predetermined response to the authenticator in accordance with the tested authorization and the captured challenge. As a result, increased security during the authentication is ensured. The invention also relates to a system comprising said type of device and an authenticator, and to a method and a computer program product for authenticating a product.

(57) **Zusammenfassung**: Es wird eine Vorrichtung zur Authentisierung eines Produktes gegenüber zumindest einem Authentisierer vorgeschlagen. Die Vorrichtung weist eine Empfangseinheit, eine Prüfeinheit und eine Sendeeinheit auf. Die Empfangseinheit ist zum Empfangen einer von dem Authentisierer gesendeten Anfragenachricht eingerichtet. Die Prüfeinheit ist zum Prüfen einer Berechtigung

[Fortsetzung auf der nächsten Seite]

WO 2013/174540 A1

des Authentisierers zum Empfangen einer Antwortnachricht auf die gesendete Anfragenachricht eingerichtet. Die Sendeeinheit ist zum Senden einer vorbestimmten Antwortnachricht an den Authentisierer in Abhängigkeit der geprüften Berechtigung und der empfangenen Anfragenachricht eingerichtet. Somit wird eine erhöhte Sicherheit bei der Authentisierung sichergestellt. Ferner werden ein System mit einer solchen Vorrichtung und mit einem Authentisierer sowie ein Verfahren und ein Computerprogrammprodukt zur Authentisierung eines Produktes vorgeschlagen.

Beschreibung

FUNKTION ZUR CHALLENGE-ABLEITUNG ZUM SCHUTZ VON KOMPONENTEN IN EINEM CHALLENGE-RESPONSE AUTHENTIFIZIERUNGSPROTOKOLL

Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zur Authentisierung eines Produktes gegenüber einem Authentisierer.

Häufig erfolgt eine Authentisierung eines Produktes, wie beispielsweise ein Gerät oder ein Objekt, mittels eines Challenge-Response-Verfahrens. Dabei wird an das zu authentisierende Produkt eine Anfragenachricht oder Challenge-Nachricht von dem Authentisierer übertragen, welche z.B. in Abhängigkeit einer Zufallszahl gebildet wird.

Daraufhin berechnet das zu authentisierende Produkt einen Response-Wert, eine Response-Nachricht oder eine Antwortnachricht, beispielsweise in Abhängigkeit eines geheimen kryptographischen Schlüssels. Diese Antwortnachricht wird an den Authentisierer zurückgeschickt, welcher die Antwortnachricht auf ihre Korrektheit hin überprüft. Da nur ein Originalprodukt oder ein Originalgerät eine korrekte Antwortnachricht berechnen kann, kann somit ein Originalprodukt bzw. ein Originalgerät zuverlässig von einer Fälschung unterschieden werden.

Ferner kann eine Challenge-Response-Authentisierung auch unter Verwendung einer physikalischen Objekteigenschaft, d.h. einer Physical Unclonable Function (PUF) erfolgen.

Physical Unclonable Functions (PUF) sind bekannt, um physikalische Objekte oder Produkte zuverlässig zu identifizieren. Eine physikalische Eigenschaft eines Produktes, z.B. ein Halbleiter-Baustein, kann dabei auch als individueller "Fingerabdruck" verwendet werden. Die Authentisierung des Produkts basiert dann darauf, dass abhängig von einer Anfragenachricht (Challenge-Wert) eine zugehörige Antwortnachricht

(Response-Wert) an den Authentisierer zurückgeliefert wird, welche durch eine physikalische Eigenschaft definierte PUF-Funktion bestimmt wird. Im Gegensatz zu einer herkömmlichen kryptographischen Challenge-Response-Authentisierung kann hierbei für die Anfragenachricht (Challenge) nicht ein beliebiger Wert (pseudo-)zufällig aus einem großen Wertebereich gewählt werden. Hierbei können nur solche Anfragenachrichten geprüft werden, für die ein zugeordneter Referenzwert in dem Authentisierer bekannt ist.

Ferner ist bekannt, eine PUF-basierte Authentisierung durchzuführen, wobei erstmalig Challenge-Response-Paare einer anderen, vertrauenswürdigen Instanz verwendet werden, um Referenzdaten für weitere Challenge-Response-Paare zu erfassen, die für spätere Authentisierungen verwendbar sind. Dies ist beispielsweise in dem Dokument US 2009/0083833 A1 beschrieben.

Des Weiteren zeigt das Dokument DE 10 2009 030 019 B3 ein System und ein Verfahren zur zuverlässigen Authentisierung eines Gerätes. Dabei wird eine Anfragenachricht mittels einer Prüferkontextinformation an eine Prüfungsvorrichtung gebunden. Daher ist es einem Angreifer erschwert, eine Identität eines Gerätes vorzutäuschen. Diese Anwendung findet Einsatz in Authentisierungsszenarien, insbesondere in der Telekommunikation, in der sensible Nachrichten ausgetauscht werden.

Demnach ist es eine Aufgabe der vorliegenden Erfindung, eine sicherere Authentisierung eines Produktes gegenüber zumindest einem Authentisierer zu schaffen.

Diese Aufgabe wird durch die unabhängigen Ansprüche gelöst. Weiterbildungen der Erfindung sind den abhängigen Ansprüchen zu entnehmen.

Demgemäß wird eine Vorrichtung zur Authentisierung eines Produktes gegenüber zumindest einem Authentisierer vorgeschlagen. Die Vorrichtung weist eine Empfangseinheit, eine Prüf-

einheit und eine Sendeeinheit auf. Die Empfangseinheit ist zum Empfangen einer von dem Authentisierer gesendeten Anfragenachricht eingerichtet. Die Prüfeinheit ist zum Prüfen einer Berechtigung des Authentisierers zum Empfangen einer Antwortnachricht auf die gesendete Anfragenachricht eingerichtet. Die Sendeeinheit ist zum Senden einer vorbestimmten Antwortnachricht an den Authentisierer in Abhängigkeit der geprüften Berechtigung und der empfangenen Anfragenachricht eingerichtet.

Die vorliegende Vorrichtung bietet eine erhöhte Sicherheit bei der Authentisierung, da nur solche Anfragenachrichten (Challenge-Nachrichten, Challenges) tatsächlich mit einer entsprechenden Antwortnachricht von der Sendeeinheit beantwortet werden, welche von einem Authentisierer gesendet wurden, der auch entsprechend berechtigt ist. Mit anderen Worten, falls eine Berechtigungsprüfung ergibt, dass die Verwendung der empfangenen Anfragenachricht oder Challenge zulässig ist, so wird die zugehörige Antwortnachricht oder Response von der Sendeeinheit an den Authentisierer gesendet.

Hierbei kann insbesondere eingeschränkt werden, welcher Authentisierer welche Challenge-Werte oder welche Challenge-Wertebereiche verwenden darf. So kann eine unkontrollierte Mehrfachverwendung von Challenge-Werten, die zu einer reduzierten Sicherheit führen könnte, verhindert werden. Weiterhin können vorzugsweise bestimmte Challenge-Werte für die Rekonstruktion eines kryptographischen Schlüssels verwendet werden, wohin andere bestimmte Challenge-Werte derselben PUF für eine Authentisierung verwendet werden. Somit kann verhindert werden, dass ein Authentisierer Antwortnachrichten erhält, die eine Rekonstruktion eines kryptographischen Schlüssels ermöglichten.

Ferner ist es auch möglich, dass mehrere Schlüssel rekonstruiert werden können, wobei jedem Schlüssel ein Challenge-Wertebereich zugeordnet ist. So können z.B. mehrere Anwendungen jeweils einen eigenen Schlüssel aus den Antwortnachrich-

ten rekonstruieren, die für jeweils zugelassene Challenge-Werte bestimmt werden. Eine physikalische PUF kann somit durch unterschiedliche Anwendungen benutzt werden.

Ein zu authentisierendes Produkt kann ein Objekt, wie beispielsweise ein Halbleiterbaustein, ein Sensorknoten, ein Steuergerät, ein bestimmter Code in einem FPGA, eine Batterie oder ein Toner bzw. eine Toner-Kartusche oder auch ein RFID-Tag auf einem Toner bzw. einer Toner-Kartusche sein.

Ein Authentisierer kann eine jede zur Kommunikation geeignete Vorrichtung sein, die an einem Challenge-Response-Verfahren teilnehmen kann. Der Authentisierer kann beispielsweise ein Authentisierungsserver sein. Die Anfragenachricht kann auch als Challenge, Challenge-Wert oder Challenge-Nachricht bezeichnet werden. Entsprechend kann die Antwortnachricht auch als Response, Response-Nachricht oder Response-Wert bezeichnet werden. Die Berechtigung kann auch als Authentisierungs-Token oder Berechtigungs-Token bezeichnet werden oder codiert sein. Beispiele hierfür sind SAML-Assertion, Attribut-Zertifikat und XML-Assertion. Damit codiert das Berechtigungs-Token die Berechtigung. Das Berechtigungs-Token ist insbesondere, um selbst gegen Manipulationen geschützt zu sein, mit einer kryptographischen Prüfsumme geschützt, oder sie wird über eine geschützte Kommunikationsverbindung bereitgestellt. Beispiele für kryptographische Prüfsummen beinhalten Message Authentication Code und digitale Signatur. Beispiele für eine solche geschützte Kommunikationsverbindung beinhalten IPsec, SSL und TLS.

Mögliche Kriterien zur Berechtigungsprüfung können eine Identitätsinformation des Authentisierers (z.B. ein Network Access Identifier (NAI), IP-Adresse, MAC-Adresse, Public Key, Public Key Hash, Prozess-ID, Hash des Programmcodes oder Dateinamen des Programmcodes). Ferner kann zur Berechtigungsprüfung eine Kontextinformation, wie aktueller Ort, aktuelle Zeit oder aktueller Betriebszustand, eingesetzt werden. Ferner kann zur Berechtigungsprüfung die Anzahl der bereits er-

folgten Verwendungen eines Challenge-Wertes verwendet werden. Auch kann der Zeitpunkt der letzten Verwendung dieses Challenge-Wertes oder die Zeitspanne seit der letzten Verwendung dieses Challenge-Wertes für die Berechtigungsprüfung herangezogen werden.

Ferner kann auch die Anzahl der noch freien, nicht verwendeten Challenge-Response-Paare eines Authentisierers oder auch die Anzahl der Prüfungen durch diesen Authentisierer in die Berechtigungsprüfung eingehen.

Die vorliegende Berechtigungsprüfung der Challenges ist insbesondere bei PUFs von Vorteil, da hier nicht beliebige Challenges verwendbar sind, sondern nur solche, für die Referenzdaten zur Prüfung vorhanden sind.

Bei einer Ausführungsform ist die Vorrichtung mit der Empfangseinheit, der Prüfeinheit und der Sendeeinheit in dem Produkt integriert.

Das Produkt, beispielsweise eine Batterie, weist die Vorrichtung oder Authentisierungsvorrichtung auf.

Bei einer weiteren Ausführungsform sind die Empfangseinheit und die Sendeeinheit in dem Produkt integriert. Ferner ist die Prüfeinheit dem Produkt derart vorgeschaltet, dass an die Empfangseinheit des Produktes gerichtete Anfragenachrichten ausschließlich über die Prüfeinheit der Vorrichtung übertragen werden können.

Bei dieser Ausführungsform kann ein herkömmliches Produkt unverändert erfindungsgemäß authentisiert werden, da die Prüfeinheit nicht Teil des Produktes ist, sondern nur diesem Produkt vorgeschaltet ist. Somit ist die Prüfeinheit als eine Vorschalteinrichtung oder vorgeordnete Challenge-Berechtigungs-Prüfvorrichtung ausgebildet.

Bei einer weiteren Ausführungsform ist die Empfangseinheit dazu eingerichtet, eine Identifikationsinformation mit der Anfragenachricht von dem Authentisierer zu empfangen. Die Prüfeinheit ist dazu eingerichtet, die Berechtigung des Authentisierers zum Empfangen der Antwortnachricht auf die gesendete Anfragenachricht in Abhängigkeit der empfangenen Identitätsinformation zu prüfen.

Die Identifikationsinformation des Authentisierers ist eine einfache Realisierung für die Berechtigungsprüfung zum Empfangen einer Antwortnachricht durch den Authentisierer.

Bei einer weiteren Ausführungsform hat die Vorrichtung eine Speichereinrichtung zum Speichern zumindest einer Berechtigungsinformation für die Berechtigung zumindest eines Authentisierers. Dabei ist die Prüfeinheit dazu eingerichtet, die Berechtigung des Authentisierers in Abhängigkeit der empfangenen Anfragenachricht und der zumindest einen gespeicherten Berechtigungsinformation zu prüfen.

Somit kann das Produkt die Berechtigung, ob die Anfragenachricht zulässig ist, anhand lokal gespeicherter Berechtigungsinformationen prüfen. So kann einem jeweiligen Authentisierer eine Menge zulässiger Challenge-Werte oder auch ein zulässiger Challenge-Wertebereich zugeordnet werden.

Bei einer weiteren Ausführungsform ist die Empfangseinheit dazu eingerichtet, eine Berechtigungsinformation mit der Anfragenachricht von dem Authentisierer zu empfangen. Hierbei ist die Prüfeinheit dazu eingerichtet, die Berechtigung des Authentisierers zum Empfangen der Antwortnachricht auf die gesendete Anfragenachricht in Abhängigkeit der empfangenen Berechtigungsinformation zu prüfen.

Die Berechtigungsinformation kann beispielsweise als ein geschütztes Berechtigungs-Token ausgebildet sein. Das Berechtigungs-Token oder Authentisierungs-Token wird von dem Authentisierer insbesondere mit der Anfragenachricht an die Vor-

richtung übertragen. Das Autorisierungs-Token bestätigt die berechtigte Nutzung eines Challenge-Wertes gegenüber der Vorrichtung.

Bei einer weiteren Ausführungsform hat die Vorrichtung eine Speichereinrichtung zum Speichern einer Anzahl von Berechtigungsinformationen für die Berechtigung einer Anzahl von Authentisierern, wobei der jeweiligen Berechtigungsinformation eine zu empfangende Anforderungsnachricht zugeordnet ist. Des Weiteren hat die Vorrichtung eine Aktualisierungseinheit zum Aktualisieren der jeweiligen Berechtigungsinformation, wenn die Empfangseinheit die der jeweiligen Berechtigungsinformation zugeordnete Anfragenachricht empfängt.

Somit kann bei der Verwendung einer Challenge zur Verifizierung, d.h. zur zweiten oder nachfolgenden Verwendung, die Berechtigung widerrufen werden, um eine weitere Verwendung dieser Challenge zu unterbinden.

Bei einer weiteren Ausführungsform ist die Aktualisierungseinheit dazu eingerichtet, die jeweilige Berechtigungsinformation derart zu aktualisieren, dass die zugehörige Berechtigung widerrufen wird, wenn die Empfangseinheit die der jeweiligen Berechtigungsinformation zugeordnete Anfragenachricht empfängt.

Durch die Sicherheitslevel-Information kann dem Authentisierer der Sicherheitslevel der aktuellen Challenge-Response-Authentisierung angezeigt werden. Die Sicherheitslevel-Information kann beispielsweise als ein Flag oder ein Trust-Value in der Antwortnachricht ausgebildet sein.

Bei einer weiteren Ausführungsform stellt die Aktualisierungseinheit eine Sicherheitslevel-Information für die empfangene Anfragenachricht in Abhängigkeit der aktualisierten Berechtigungsinformation bereit. Dabei ist die Sendeeinheit dazu eingerichtet, die bereitgestellte Sicherheitslevel-

Information mit der vorbestimmten Antwortnachricht an den Authentisierer zu senden.

Insbesondere kann das System mehrere PUF-Authentisierungsserver aufweisen, denn in einem solchen Fall kann erfindungsgemäß kontrolliert werden, welcher PUF-Authentisierungsserver welche Challenge-Werte verwenden darf. Auch kann erfindungsgemäß eingeschränkt werden, wann ein bestimmter Authentisierungsserver ein Produkt oder Objekt authentisieren kann, z.B. nur solange, bis dessen Haltbarkeitsdatum nicht abgelaufen ist. Auch kann ein Objekt gegebenenfalls nur dann authentisiert werden, solange es sich an einem bestimmten Ort oder einem bestimmten Gebiet befindet. Diese Informationen können aus der Kontext-Information in die Berechtigungsprüfung mit eingehen.

Bei einer weiteren Ausführungsform ist die Prüfeinheit dazu eingerichtet, vor der Prüfung der Berechtigung des Authentisierers das Format und/oder den Inhalt der empfangenen Anfragenachricht zu prüfen.

Die jeweilige Einheit, Empfangseinheit, Prüfeinheit und Sendeeinheit, kann hardwaretechnisch und/oder auch softwaretechnisch implementiert sein. Bei einer hardwaretechnischen Implementierung kann die jeweilige Einheit als Vorrichtung oder als Teil einer Vorrichtung, zum Beispiel als Computer oder als Mikroprozessor ausgebildet sein. Bei einer softwaretechnischen Implementierung kann die jeweilige Einheit als Computerprogrammprodukt, als eine Funktion, als eine Routine, als Teil eines Programmcodes oder als ausführbares Objekt ausgebildet sein.

Weiter wird ein System mit zumindest einem Authentisierer und einer wie oben beschriebenen Vorrichtung zur Authentisierung eines Produktes gegenüber dem zumindest einen Authentisierer vorgeschlagen. Der Authentisierer ist zum Senden einer Anfragenachricht an die Vorrichtung und zum Empfangen und Prüfen

einer als Antwort auf die gesendete Anfragenachricht empfangenen Antwortnachricht von der Vorrichtung eingerichtet.

Bei einer Weiterbildung sind der Authentisierer und die Vorrichtung derart eingerichtet, dass sich der Authentisierer gegenüber der Vorrichtung authentisiert.

Bei einer weiteren Weiterbildung hat das System zumindest einen ersten Authentisierer und einen zweiten Authentisierer Dabei ist der erste Authentisierer dazu eingerichtet, eine Berechtigung zum Empfangen einer Antwortnachricht von der Vorrichtung durch ein Senden einer Anfragenachricht an die Vorrichtung und durch ein Empfangen einer entsprechenden Antwortnachricht von der Vorrichtung zu generieren und die generierte Berechtigung mit einer integritätsgeschützten Weiterleitungsnachricht an den zweiten Authentisierer weiterzuleiten.

Ferner wird ein Verfahren zur Authentisierung eines Produktes gegenüber zumindest einem Authentisierer vorgeschlagen. In einem ersten Schritt wird eine von dem Authentisierer gesendete Anfragenachricht empfangen. In einem zweiten Schritt wird eine Berechtigung des Authentisierers zum Empfangen einer Antwortnachricht auf die gesendete Anfragenachricht geprüft. In einem dritten Schritt wird eine vorbestimmte Antwortnachricht an den Authentisierer in Abhängigkeit der geprüften Berechtigung und der empfangenen Anfragenachricht gesendet.

Weiterhin wird ein Computerprogrammprodukt vorgeschlagen, welches auf einer programmgesteuerten Einrichtung die Durchführung des wie oben erläuterten Verfahrens veranlasst.

Ein Computerprogrammprodukt wie ein Computerprogramm-Mittel kann beispielsweise als Speichermedium, wie Speicherkarte, USB-Stick, CD-ROM, DVD oder auch in Form einer herunterladbaren Datei von einem Server in einem Netzwerk bereitgestellt oder geliefert werden. Dies kann zum Beispiel in einem draht-

losen Kommunikationsnetzwerk durch die Übertragung einer entsprechenden Datei mit dem Computerprogrammprodukt oder dem Computerprogramm-Mittel erfolgen.

Außerdem wird ein Datenträger mit einem gespeicherten Computerprogramm mit Befehlen vorgeschlagen, welche die Durchführung des wie oben erläuterten Verfahrens auf einer programmgesteuerten Einrichtung veranlassen.

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Zeichnungen näher erläutert werden.

Dabei zeigen:

Fig. 1 ein Blockschaltbild eines ersten Ausführungsbeispiels einer Vorrichtung zur Authentisierung eines Produkts;

Fig. 2 ein Blockschaltbild eines zweiten Ausführungsbeispiels einer Vorrichtung zur Authentisierung eines Produkts;

Fig. 3 ein Blockschaltbild eines dritten Ausführungsbeispiels einer Vorrichtung zur Authentisierung eines Produkts;

Fig. 4 ein Blockschaltbild eines Ausführungsbeispiels eines Systems zur Authentisierung eines Produkts mit zwei Authentisierungsservern; und

Fig. 5 ein Ablaufdiagramm eines Ausführungsbeispiels eines Verfahrens zur Authentisierung eines Produkts.

In den Figuren sind gleiche oder funktionsgleiche Elemente mit denselben Bezugszeichen versehen worden, sofern nichts anderes angegeben ist.

Fig. 1 zeigt ein Blockschaltbild eines ersten Ausführungsbeispiels einer Vorrichtung 10 zur Authentisierung eines Produkts 1 gegenüber einem Authentisierer 2. Die Vorrichtung 10 und der Authentisierer 2 sind über eine Kommunikationsverbindung gekoppelt.

In dem Ausführungsbeispiel der Fig. 1 ist die Vorrichtung 10 Teil des zu authentisierenden Produktes 1.

Die Vorrichtung 10 hat eine Empfangseinheit 11, eine Prüfeinheit 12 und eine Sendeeinheit 13.

Die Empfangseinheit 11 ist dazu eingerichtet, eine von dem Authentisierer 2 gesendete Anfragenachricht C zu empfangen. Die Prüfeinheit 12 prüft die Berechtigung B des Authentisierers 2 zum Empfangen einer Antwortnachricht R auf die gesendete Anfragenachricht C.

Die Sendeeinheit 13 ist dazu eingerichtet, eine vorbestimmte Antwortnachricht R an den Authentisierer 2 in Abhängigkeit der geprüften Berechtigung B und der empfangenen Anfragenachricht C zu senden. D.h., dass die geprüfte Berechtigung B indiziert, ob an den Authentisierer 2 eine Antwortnachricht R gesendet werden soll oder nicht. Nur bei einer positiven Berechtigung B des Authentisierers 2 wird eine solche Antwortnachricht R an diesen gesendet. Bei einer positiven Berechtigung des Authentisierers 2 wird die Art der Antwortnachricht R insbesondere in Abhängigkeit der geprüften Berechtigung B und/oder der empfangenen Anfragenachricht C bestimmt.

Mit der Anfragenachricht C kann der Authentisierer 2 eine Identifikationsinformation zu seiner eigenen Identifikation gegenüber der Vorrichtung 10 an diese übertragen. Die Identi-

fikationsinformation kann zur Berechtigungsprüfung des Authentisierers 2 verwendet werden.

Alternativ oder zusätzlich kann der Authentisierer 2 eine Berechtigungsinformation mit der Anfragenachricht C an die Empfangseinheit 11 der Vorrichtung 10 übertragen. Die Berechtigungsinformation kann direkt indizieren, dass der Authentisierer 2 zum Empfangen von Antwortnachrichten R von der Vorrichtung 10 berechtigt ist. Mit anderen Worten, die Prüfeinheit 12 prüft dann die Berechtigung B des Authentisierers 2 zum Empfangen der Antwortnachricht R auf die gesendete Anfragenachricht C in Abhängigkeit der empfangenen Berechtigungsinformation.

Zusätzlich kann die Prüfeinheit 12 dazu eingerichtet sein, vor der Prüfung der Berechtigung B des Authentisierers 2 das Format der empfangenen Anfragenachricht C zu prüfen. Beispielsweise wird die Berechtigung B des Authentisierers 2 von der Prüfeinheit 12 nur dann geprüft, wenn das Format der empfangenen Anfragenachricht C einem vorbestimmten Format entspricht.

In Fig. 2 ist ein Blockschaltbild eines zweiten Ausführungsbeispiels einer Vorrichtung 10 zur Authentisierung eines Produktes 1 gegenüber einem Authentisierer 2 dargestellt.

Das zweite Ausführungsbeispiel der Fig. 2 unterscheidet sich von dem ersten Ausführungsbeispiel der Fig. 1 insbesondere dahingehend, dass die Empfangseinheit 11 und die Sendeeinheit 13 der Vorrichtung 10 in dem zu authentisierenden Produkt 1 integriert sind, die Prüfeinheit 12 aber nicht Teil des Produktes 1 ist, sondern diesem vorgeschaltet ist. Die Prüfeinheit 12 ist dem Produkt 1 derart vorgeschaltet, dass an die Empfangseinheit 11 des Produktes 1 gerichtete Anfragenachrichten C ausschließlich über die Prüfeinheit 12 der Vorrichtung 10 übertragen werden können. Dazu kann die Prüfeinheit 12 ein Prüfmittel 15 aufweisen, welches die Berechtigung B des Authentisierers 2 prüft. Bei einer positiven Berechtigung

B überträgt das Prüfmittel 15 ein Berechtigungssignal B an ein Schaltmittel 16, welches dann die Kommunikationsverbindung zwischen der Sendeeinheit 13 der Vorrichtung 10 und dem Authentisierer 2 bewerkstelligt. Bei Feststellen einer unzulässigen Berechtigung durch das Prüfmittel 15 steuert das Prüfmittel 15 das Schaltmittel 16 derart an, dass die Kommunikationsverbindung zwischen der Sendeeinheit 13 und dem Authentisierer 2 unterbrochen ist.

Ferner ist in dem zweiten Ausführungsbeispiel der Fig. 2 eine Speichereinrichtung 14 zum Speichern zumindest einer Berechtigungsinformation Ref für die Berechtigung des Authentisierers 2 vorgesehen. Dann kann die Prüfeinheit 12 die Berechtigung B des Authentisierers 2 in Abhängigkeit der empfangenen Anfragenachricht C und der gespeicherten Berechtigungsinformation Ref prüfen. Insbesondere können die gespeicherten Berechtigungsinformationen Ref auch als Referenzwerte oder Referenzdaten bezeichnet werden.

Ferner kann die Speichereinrichtung 14 auch zum Speichern einer Mehrzahl von Berechtigungsinformationen Ref für die Berechtigung einer Mehrzahl von Authentisierern 2 eingerichtet werden, wobei der jeweilige Berechtigungsinformation Ref eine zu empfangene Anforderungsnachricht C zugeordnet ist.

Fig. 3 zeigt ein Blockschaltbild eines dritten Ausführungsbeispiels einer Vorrichtung 10 zur Authentisierung eines Produktes 1. Das dritte Ausführungsbeispiel der Fig. 3 basiert auf dem ersten Ausführungsbeispiel der Fig. 1, wobei die Vorrichtung 10 der Fig. 3 zusätzlich eine Speichereinrichtung 14 und eine Aktualisierungseinheit 17 aufweist. Die Speichereinrichtung 14 der Vorrichtung 10 ist zum Speichern einer Anzahl von Berechtigungsinformationen Ref für die Berechtigung einer Anzahl von Authentisierern 2 eingerichtet, wobei der jeweiligen Berechtigungsinformation Ref eine zu empfangene Anforderungsnachricht C zugeordnet ist.

Die Speichereinrichtung 14 ist insbesondere zwischen der Aktualisierungseinheit 17 und der Prüfeinheit 12 gekoppelt. Die Aktualisierungseinheit 17 ist dazu eingerichtet, die jeweilige Berechtigungsinformation Ref der Speichereinrichtung 14 mittels eines Aktualisierungssignals A zu aktualisieren, wenn die Empfangseinheit 11 die der jeweiligen Berechtigungsinformation Ref zugeordnete Anfragenachricht C von einem Authentisierer 2 empfängt. Insbesondere kann die Aktualisierungseinrichtung 17 auch dazu eingerichtet sein, die jeweilige Berechtigungsinformation Ref derart zu aktualisieren, dass die zugehörige Berechtigung B widerrufen wird, wenn die Empfangseinheit 11 die der jeweiligen Berechtigungsinformation Ref zugeordnete Anfragenachricht C empfängt.

Weiter kann die Aktualisierungseinheit 17 dazu eingerichtet sein, eine Sicherheitslevel-Information für die empfangene Anfragenachricht C in Abhängigkeit der aktualisierten Berechtigungsinformation Ref zu generieren. Dann kann die Sendeeinheit 13 dazu eingerichtet werden, die generierte Sicherheitslevel-Information mit der vorbestimmten Antwortnachricht R an den Authentisierer 2 zu senden.

Fig. 4 zeigt ein Blockschaltbild eines Ausführungsbeispiels eines Systems zur Authentisierung eines Produktes 1 mit zwei Authentisierungsservern 21, 22. Dabei führt ein erster Authentisierungsserver 21 eine so genannte Enrollment-Phase (Schritte 401 – 403) durch, in welcher Challenge-Response-Paare aus Challenges und Responses generiert werden. Ein Challenge-Response-Paar indiziert dabei eine Berechtigung des anfragenden Authentisierungsservers. Diese Berechtigungen kann der erste Authentisierungsserver 21 dem weiteren zweiten Authentisierungsserver 22 weiterleiten oder delegieren. In einer der Enrollment-Phase (Schritte 401 – 403) folgenden Anwendungsphase (Schritte 404 – 408) kann der zweite Authentisierungsserver 22 die delegierte Berechtigung des Authentisierungsservers 21 nutzen. Dies wird im Folgenden mit Bezug zu Fig. 4 im Detail erläutert.

In Schritt 401 sendet der erste Authentisierungsserver 21 eine Challenge C an die Vorrichtung 10. Die Vorrichtung 10 antwortet mit einer Response R in Schritt 402. In Schritt 403 sendet der erste Authentifizierungsserver 21 eine Weiterleitungsnachricht W mit der Berechtigung B zum Empfangen von Responses von der Vorrichtung 10 an den zweiten Authentisierungsserver 22. In Schritt 404 generiert der zweite Authentisierungsserver 22 eine Challenge C mit der übermittelten Berechtigung B. In Schritt 405 überträgt der zweite Authentisierungsserver 22 die generierte Challenge C an die Vorrichtung 10. In Schritt 406 prüft die Vorrichtung 10 die empfangene Berechtigung, die von dem ersten Authentisierungsserver 21 an den zweiten Authentisierungsserver 22 delegiert wurde. Da diese Berechtigung zulässig ist, weil sie in der Enrollment-Phase generiert wurde, kann die Vorrichtung 10 eine Response R im Schritt 406 an den zweiten Authentisierungsserver 22 senden. In Schritt 407 verifiziert der zweite Authentisierungsserver 22 die empfangene Response R.

In Fig. 5 ist ein Ablaufdiagramm eines Ausführungsbeispiels eines Verfahrens zur Authentisierung eines Produkts gegenüber einem Authentisierer dargestellt.

In Schritt 501 wird eine von dem Authentisierer gesendete Anfragenachricht von dem Produkt empfangen.

In Schritt 502 wird eine Berechtigung des Authentisierers zum Empfangen einer Antwortnachricht auf die gesendete Anfragenachricht von dem Produkt geprüft.

In Schritt 503 wird eine vorbestimmte Antwortnachricht von dem Produkt an den Authentisierer in Abhängigkeit der geprüften Berechtigung und der empfangenen Anfragenachricht gesendet.

Obwohl die Erfindung im Detail durch das bevorzugte Ausführungsbeispiel näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele einge-

schränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

Patentansprüche

1. Vorrichtung (10) zur Authentisierung eines Produktes (1) gegenüber zumindest einem Authentisierer (2), mit:
einer Empfangseinheit (11) zum Empfangen einer von dem Authentisierer (2) gesendeten Anfragenachricht (C),
einer Prüfeinheit (12) zum Prüfen einer Berechtigung des Authentisierers (2) zum Empfangen einer Antwortnachricht (R) auf die gesendete Anfragenachricht (C), und
einer Sendeeinheit (13) zum Senden einer vorbestimmten Antwortnachricht (R) an den Authentisierer (2) in Abhängigkeit der geprüften Berechtigung (B) und der empfangenen Anfragenachricht (C).

2. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass die Vorrichtung (10) mit der Empfangseinheit (11), der Prüfeinheit (12) und der Sendeeinheit (13) in dem Produkt (1) integriert ist.

3. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass die Empfangseinheit (11) und die Sendeeinheit (13) in dem Produkt (1) integriert sind und die Prüfeinheit (12) dem Produkt (1) derart vorgeschaltet ist, dass an die Empfangseinheit (11) des Produktes (1) gerichtete Anfragenachrichten (C) ausschließlich über die Prüfeinheit (12) der Vorrichtung (10) übertragbar sind.

4. Vorrichtung nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass die Empfangseinheit (11) dazu eingerichtet ist, eine Identifikationsinformation mit der Anfragenachricht (C) von dem Authentisierer (2) zu empfangen, und
dass die Prüfeinheit (12) dazu eingerichtet ist, die Berechtigung (B) des Authentisierers (2) zum Empfangen der Antwortnachricht (R) auf die gesendete Anfragenachricht (C) in Abhängigkeit der empfangenen Identitätsinformation zu prüfen.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, gekennzeichnet durch eine Speichereinrichtung (14) zum Speichern zumindest einer Berechtigungsinformation (Ref) für die Berechtigung zumindest eines Authentisierers (2), wobei die Prüfeinheit (12) dazu eingerichtet ist, die Berechtigung (B) des Authentisierers (2) in Abhängigkeit der empfangenen Anfragenachricht (C) und der zumindest einen gespeicherten Berechtigungsinformation (Ref) zu prüfen.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Empfangseinheit (11) dazu eingerichtet ist, eine Berechtigungsinformation mit der Anfragenachricht (C) von dem Authentisierer (2) zu empfangen, und dass die Prüfeinheit (12) dazu eingerichtet ist, die Berechtigung (B) des Authentisierers (2) zum Empfangen der Antwortnachricht (R) auf die gesendete Anfragenachricht (C) in Abhängigkeit der empfangenen Berechtigungsinformation zu prüfen.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, gekennzeichnet durch eine Speichereinrichtung (14) zum Speichern einer Anzahl von Berechtigungsinformationen (Ref) für die Berechtigung einer Anzahl von Authentisierern (2), wobei der jeweiligen Berechtigungsinformation (Ref) eine zu empfangende Anforderungsnachricht (C) zugeordnet ist, und eine Aktualisierungseinheit (17) zum Aktualisieren der jeweiligen Berechtigungsinformation (Ref), wenn die Empfangseinheit (11) die der jeweiligen Berechtigungsinformation (Ref) zugeordnete Anfragenachricht (C) empfängt.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Aktualisierungseinheit (17) dazu eingerichtet ist, die jeweilige Berechtigungsinformation (Ref) derart zu aktua-

lisieren, dass die zugehörige Berechtigung (B) widerrufen wird, wenn die Empfangseinheit (11) die der jeweiligen Berechtigungsinformation (Ref) zugeordnete Anfragenachricht (C) empfängt.

9. Vorrichtung nach Anspruch 7 oder 8,
dadurch gekennzeichnet,
dass die Aktualisierungseinheit (17) eine Sicherheitslevel-Information für die empfangene Anfragenachricht (C) in Abhängigkeit der aktualisierten Berechtigungsinformation (Ref) bereitstellt, wobei die Sendeeinheit (13) dazu eingerichtet ist, die bereitgestellte Sicherheitslevel-Information mit der vorbestimmten Antwortnachricht (R) an den Authentisierer (2) zu senden.

10. Vorrichtung nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet,
dass die Prüfeinheit (12) dazu eingerichtet ist, vor der Prüfung der Berechtigung (B) des Authentisierers (2) das Format der empfangenen Anfragenachricht (C) zu prüfen.

11. System, mit:
einer Vorrichtung (10) zur Authentisierung eines Produktes (1) gegenüber zumindest einem Authentisierer (2) nach einem der Ansprüche 1 bis 10, und
zumindest einem Authentisierer (2) zum Senden einer Anfragenachricht (C) an die Vorrichtung (10) und zum Empfangen und Prüfen einer als Antwort auf die gesendete Anfragenachricht (C) empfangenen Antwortnachricht (R) von der Vorrichtung (10).

12. System nach Anspruch 11,
dadurch gekennzeichnet,
dass der Authentisierer (2) und die Vorrichtung (10) derart eingerichtet sind, dass sich der Authentisierer (2) gegenüber der Vorrichtung (10) authentisiert.

13. System nach Anspruch 11 oder 12,

dadurch gekennzeichnet,
dass ein erster Authentisierer (21) und ein zweiter Authentisierer (22) vorgesehen sind, wobei der erste Authentisierer (21) dazu eingerichtet ist, eine Berechtigung (B) zum Empfangen einer Antwortnachricht (R) von der Vorrichtung (10) durch ein Senden einer Anfragenachricht (C) an die Vorrichtung (10) und durch ein Empfangen einer entsprechenden Antwortnachricht (R) von der Vorrichtung (10) zu generieren und die generierte Berechtigung (B) mit einer integritätsgeschützten Weiterleitungsnachricht (W(B)) an den zweiten Authentisierer (22) weiterzuleiten.

14. Verfahren zur Authentisierung eines Produktes gegenüber zumindest einem Authentisierer, mit den Schritten:
Empfangen (501) einer von dem Authentisierer gesendeten Anfragenachricht,
Prüfen (502) einer Berechtigung des Authentisierers zum Empfangen einer Antwortnachricht auf die gesendete Anfragenachricht, und
Senden (503) einer vorbestimmten Antwortnachricht an den Authentisierer in Abhängigkeit der geprüften Berechtigung und der empfangenen Anfragenachricht.

15. Computerprogrammprodukt, welches auf einer programmgesteuerten Einrichtung die Durchführung eines Verfahrens nach Anspruch 14 veranlasst.

FIG 1

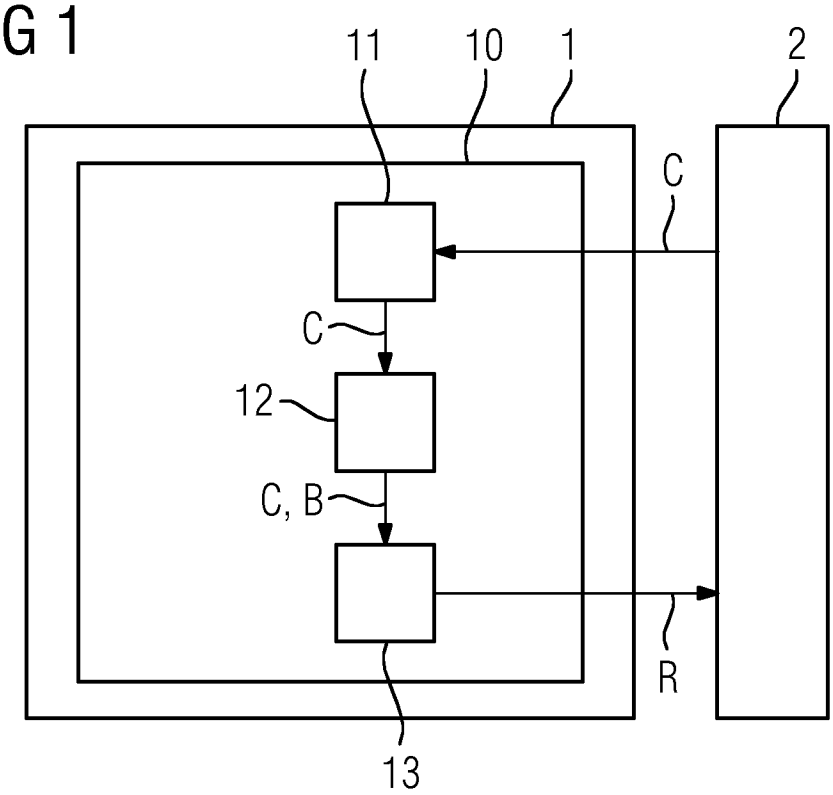


FIG 2

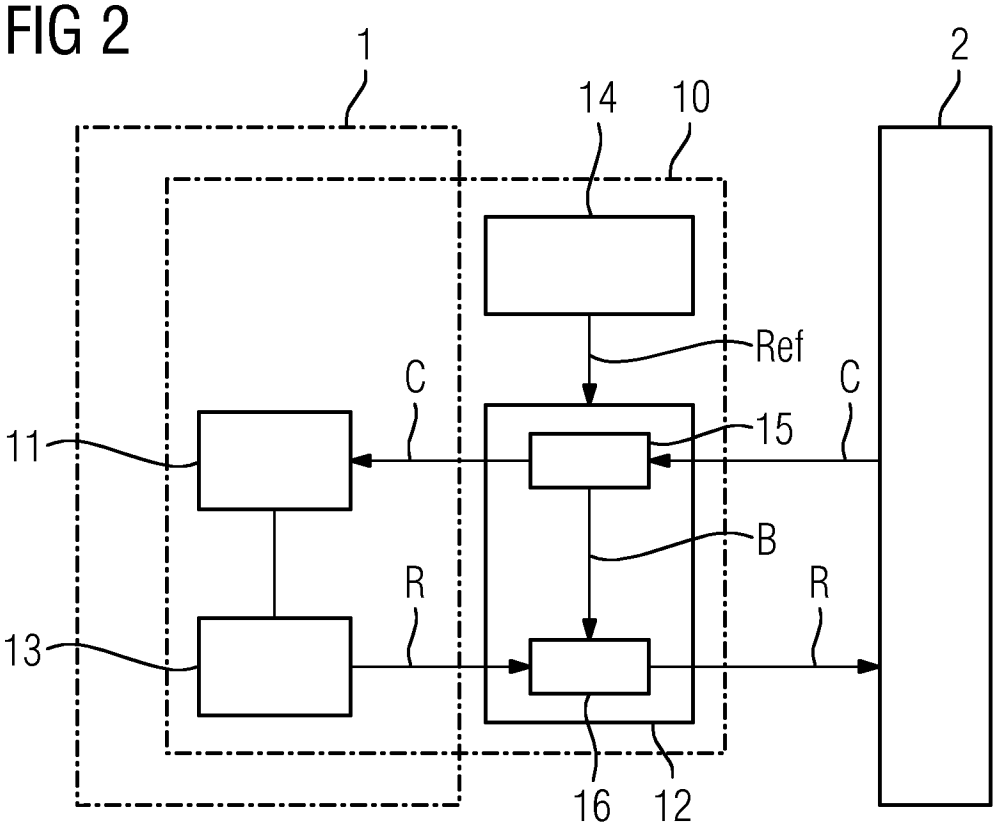


FIG 3

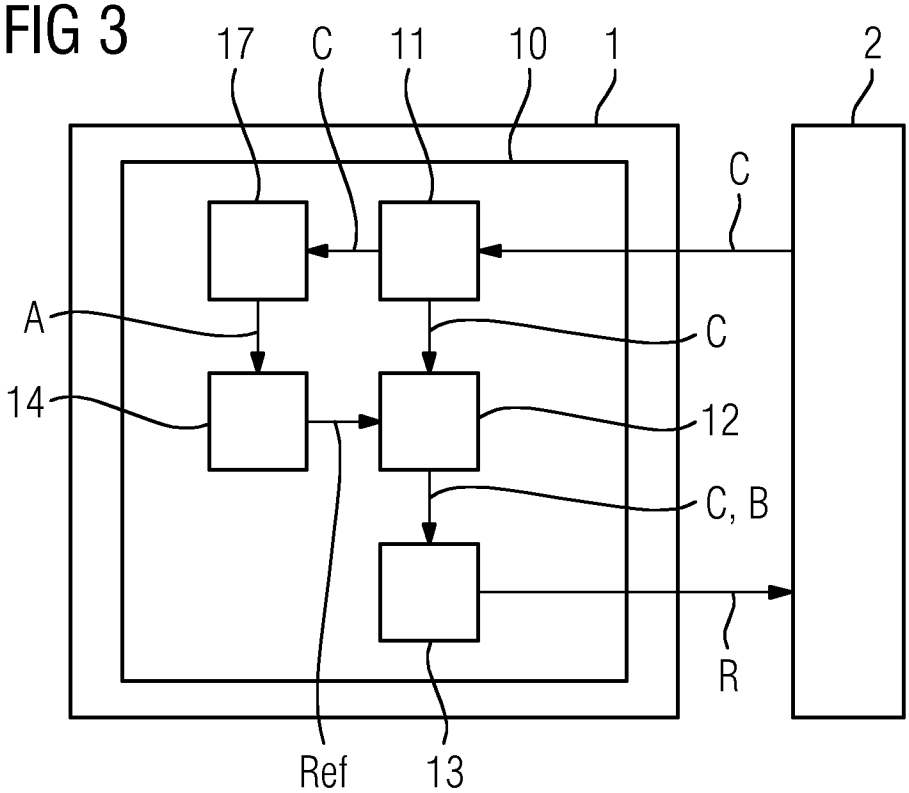


FIG 4

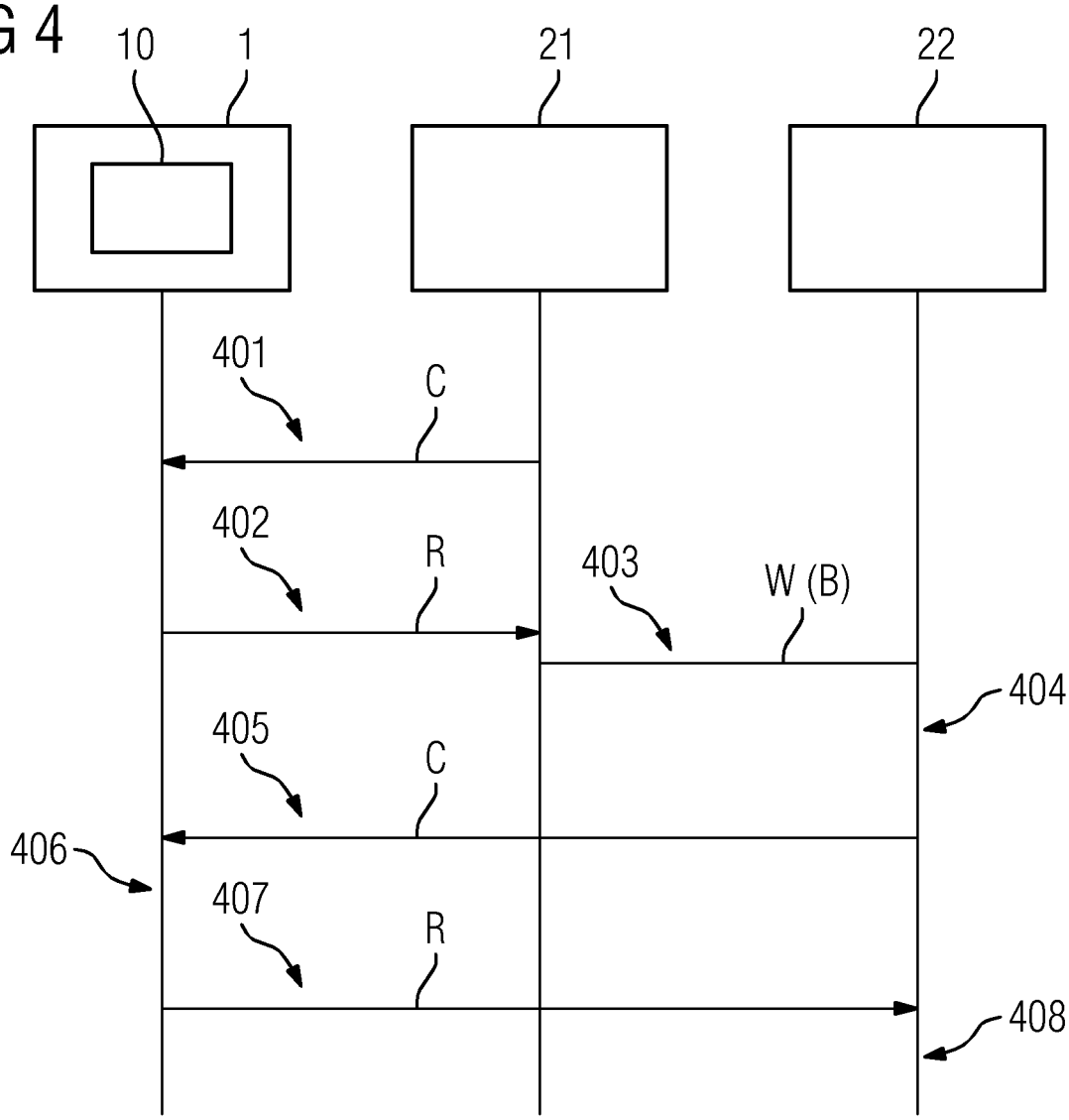
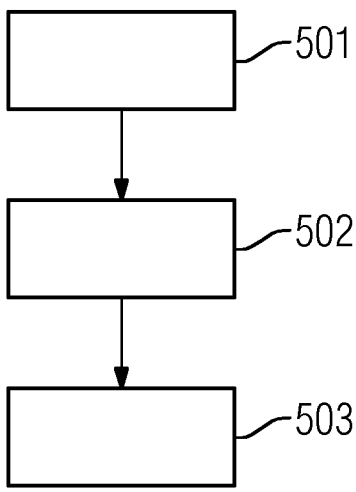


FIG 5



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/055923

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 H04L29/06
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)
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, PAJ, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Rainer Falk ET AL: "Protecting Remote Component Authentication", SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies, 27 August 2011 (2011-08-27), 27 August 2011 (2011-08-27), pages 19-24, XP055078870, Nice/Saint Laurent du Var, France ISBN: 978-1-61-208146-5 Retrieved from the Internet: URL:http://www.thinkmind.org/download.php?articleid=sec_v5_n12_2012_3 [retrieved on 2013-09-11]	1-6,9-15
Y	the whole document	7,8

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
16 September 2013	23/09/2013

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	Bec, Thierry

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2009 030019 B3 (SIEMENS AG [DE]) 30 December 2010 (2010-12-30) cited in the application	1-6, 10-15
A	abstract paragraph [0001] - paragraph [0002] paragraph [0005] paragraph [0010] - paragraph [0041] paragraph [0082] - paragraph [0098] pages 1,4,5	7-9

Y	WO 2007/038896 A2 (PRIVASPHERE AG [CH]; HAUSER RALF [CH]) 12 April 2007 (2007-04-12)	7,8
A	page 3, line 18 - page 4, last line page 8, line 24 - page 9, line 21 page 19, line 19 - page 22, line 24	1-6, 10-15

A	MOHAMAD BADRA ET AL: "Random Values, Nonce and Challenges: Semantic Meaning versus Opaque and Strings of Data", VEHICULAR TECHNOLOGY CONFERENCE FALL (VTC 2009-FALL), 2009 IEEE 70TH, IEEE, PISCATAWAY, NJ, USA, 20 September 2009 (2009-09-20), pages 1-5, XP031600319, ISBN: 978-1-4244-2514-3 paragraph [00II] - paragraph [000V]	1-15

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/055923

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102009030019 B3	30-12-2010	DE 102009030019 B3	30-12-2010
		EP 2446390 A1	02-05-2012
		US 2012102319 A1	26-04-2012
		WO 2010149400 A1	29-12-2010
WO 2007038896 A2	12-04-2007	AT 527797 T	15-10-2011
		JP 2009510955 A	12-03-2009
		KR 20080059617 A	30-06-2008
		US 2008212771 A1	04-09-2008
		WO 2007038896 A2	12-04-2007

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/055923

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/32 H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
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, PAJ, COMPENDEX, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	Rainer Falk ET AL: "Protecting Remote Component Authentication", SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies, 27. August 2011 (2011-08-27), 27. August 2011 (2011-08-27), Seiten 19-24, XP055078870, Nice/Saint Laurent du Var, France ISBN: 978-1-61-208146-5 Gefunden im Internet: URL:http://www.thinkmind.org/download.php?articleid=sec_v5_n12_2012_3 [gefunden am 2013-09-11]	1-6,9-15
Y	das ganze Dokument	7,8

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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
16. September 2013	23/09/2013

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	Bec, Thierry

3

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2009 030019 B3 (SIEMENS AG [DE]) 30. Dezember 2010 (2010-12-30) in der Anmeldung erwähnt	1-6, 10-15
A	Zusammenfassung Absatz [0001] - Absatz [0002] Absatz [0005] Absatz [0010] - Absatz [0041] Absatz [0082] - Absatz [0098] Seiten 1,4,5	7-9

Y	WO 2007/038896 A2 (PRIVASPHERE AG [CH]; HAUSER RALF [CH]) 12. April 2007 (2007-04-12)	7,8
A	Seite 3, Zeile 18 - Seite 4, letzte Zeile Seite 8, Zeile 24 - Seite 9, Zeile 21 Seite 19, Zeile 19 - Seite 22, Zeile 24	1-6, 10-15

A	MOHAMAD BADRA ET AL: "Random Values, Nonce and Challenges: Semantic Meaning versus Opaque and Strings of Data", VEHICULAR TECHNOLOGY CONFERENCE FALL (VTC 2009-FALL), 2009 IEEE 70TH, IEEE, PISCATAWAY, NJ, USA, 20. September 2009 (2009-09-20), Seiten 1-5, XP031600319, ISBN: 978-1-4244-2514-3 Absatz [00II] - Absatz [000V]	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/055923

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102009030019 B3	30-12-2010	DE 102009030019 B3	30-12-2010
		EP 2446390 A1	02-05-2012
		US 2012102319 A1	26-04-2012
		WO 2010149400 A1	29-12-2010
WO 2007038896 A2	12-04-2007	AT 527797 T	15-10-2011
		JP 2009510955 A	12-03-2009
		KR 20080059617 A	30-06-2008
		US 2008212771 A1	04-09-2008
		WO 2007038896 A2	12-04-2007