

(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
5. Oktober 2017 (05.10.2017)



(10) Internationale Veröffentlichungsnummer
WO 2017/167526 A1

- (51) Internationale Patentklassifikation:
G07C 13/00 (2006.01) **H04L 9/32** (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2017/054745
- (22) Internationales Anmeldedatum:
1. März 2017 (01.03.2017)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2016 205 121.0 29. März 2016 (29.03.2016) DE
- (71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
[DE/DE]; Werner-von-Siemens-Straße 1, 80333 München (DE).
- (72) Erfinder: **GERKEN, Stefan**; Lammer Heide 251, 38116 Braunschweig (DE). **ECKELMANN-WENDT, Uwe**; Am Forst 11, 38302 Wolfenbüttel (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, 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).

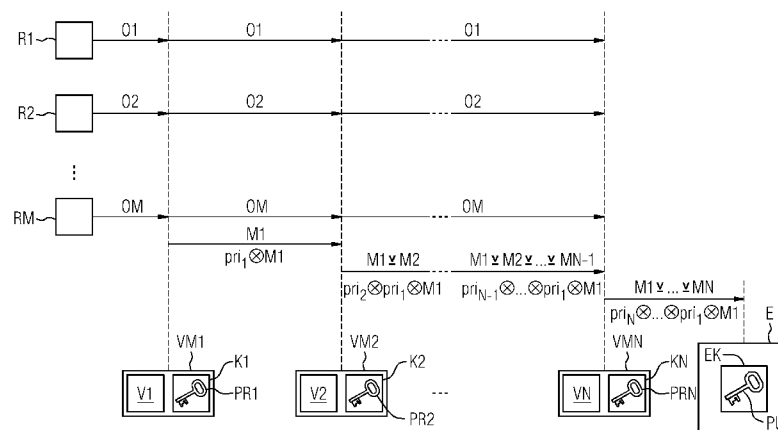
Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

(54) Title: METHOD FOR VOTING USING CONCATENATED SIGNATURES

(54) Bezeichnung : VERFAHREN ZUM VOTING MIT VERKETTETEN SIGNATUREN

FIG 1



(57) Abstract: A method for voting using concatenated signatures, wherein a plurality M of replicants (R1, R2, RM) for generating M redundant messages, where $M \geq 2$, and a plurality N of voter modules (VM1, VM2, VMN), where $N \geq 2$, are provided, wherein each voter module (VM1, VM2, VMN) has a voter (V1, V2, VN) for voting the redundant messages (O1, O2, ON) and a crypto unit (K1, K2, KN) with a private key fragment (PR1, PR2, PRN) for signing a message. The redundant messages (O1, O2, OM) of the replicants are transmitted to each voter module (VM1, VM2, VMN), so that the voter (V1, V2, VN) of each voter module (VM1, VM2, VMN) generates a voted message (M1, M2, MN) on the basis of the redundant messages. N private key fragments (PR1, PR2, PRN) are used to generate signatures for the voted messages that are checked by a public key (PU) of a reception unit (E). In the event of a successful check, the repeatedly voted message is accepted. Further, an apparatus for performing the method for voting using concatenated signatures is proposed.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



Verfahren zum Voting mit verketteten Signaturen, wobei eine Mehrzahl M von Replikanten (R1, R2, RM) zur Erzeugung von M redundanten Nachrichten mit $M \geq 2$ sowie eine Mehrzahl N von Votermodulen (VM1, VM2, VMN) mit $N \geq 2$ vorgesehen ist, wobei jedes Votermodul (VM1, VM2, VMN) einen Voter (V1, V2, VN) zum Voting der redundanten Nachrichten (O1, O2, ON) sowie eine Kryptoeinheit (K1, K2, KN) mit privatem Teilschlüssel (PR1, PR2, PRN) zum Signieren einer Nachricht aufweist. Die redundanten Nachrichten (O1, O2, OM) der Replikanten werden an jedes Votermodul (VM1, VM2, VMN) übermittelt, so dass der Voter (V1, V2, VN) jedes Votermoduls (VM1, VM2, VMN) eine gevotete Nachricht (M1, M2, MN) auf Basis der redundanten Nachrichten erzeugt. Es werden mit Hilfe von N privaten Teilschlüsseln (PR1, PR2, PRN) Signaturen der gevoteten Nachrichten erzeugt, die von einem öffentlichen Schlüssel (PU) einer Empfangseinheit (E) geprüft werden. Bei erfolgreicher Prüfung wird die mehrfach gevotete Nachricht akzeptiert. Ferner wird eine Vorrichtung zur Durchführung des Verfahrens zum Voting mit verketteten Signaturen vorgeschlagen.

Beschreibung

Verfahren zum Voting mit verketteten Signaturen

- 5 Die Erfindung betrifft ein Verfahren zum Voting mit verketteten Signaturen sowie eine Vorrichtung zum Ausführen des Verfahrens.

10 Sicherheitstechnische Daten müssen mehrfach redundant identisch berechnet worden sein, wobei jede Berechnungsart auch als Kanal oder Replikant bezeichnet wird, oder zumindest redundant geprüft worden sein, um als signaltechnisch sicher zu gelten. Dies gilt für alle Sicherheitsstufen gemäß einschlägiger Normen (z.B. IEC61508, CENELEC EN50129). Aus der mehr-

15 fachen Berechnung eines Datums wird durch Voting eine signaltechnisch sichere Nachricht. Beim Voting werden von einem Voter mehrere eingehende Daten bzw. Nachrichten miteinander verglichen und ein „richtiges“ Datum ausgegeben. Ein Voter kann beispielsweise einen Mehrheitsentscheid durchführen,

20 d.h. wenn eine Mehrheit von Eingängen eines Voters eine bestimmte Nachricht anzeigt, dann wird diese Nachricht ausgegeben. Bisher wurde für das Voting ein spezielles signaltechnisch sicheres Gerät oder eine signaltechnisch sichere Komponente verwendet. Es wäre jedoch günstiger für das Gesamtsystem,

25 wenn die Voter auch auf einem signaltechnisch nicht sicheren Gerät ausgeführt werden können, idealerweise auf dem selben Gerät wie die gevoteten Nachrichten. Bisher hat man zumindest in den höheren Sicherheitsniveaus jedoch ausschließlich proprietäre Hardware für Voter verwendet, die

30 nicht allgemeinen Standards entsprechen. Kommerzielle nicht signaltechnisch sichere Hardware konnte bisher nicht eingesetzt werden.

Die Aufgabe besteht darin, ein Verfahren zum Voting von Nachrichten zu entwickeln, das hohen Sicherheitsanforderungen gerecht wird und auf kommerzieller Hardware ausgeführt werden kann.

35

Das erfindungsgemäße Verfahren zum Voting mit verketteten Signaturen umfasst grundsätzlich folgende Schritte: In einem Schritt a) wird eine Mehrzahl M von Replikanten zur Erzeugung von M redundanten Nachrichten bereitgestellt, wobei $M \geq 2$. In einem Schritt b) wird eine Mehrzahl N von Votermodulen mit $N \geq 2$ bereitgestellt, wobei jedes Votermodul einen Voter zum Voting der redundanten Nachrichten sowie eine Kryptoeinheit mit privatem Teilschlüssel zum Signieren einer Nachricht aufweist. In einem Schritt c) werden die redundanten Nachrichten der Replikanten an jedes Votermodul übergeben, so dass der Voter jedes Votermoduls eine gevotete Nachricht auf Basis der redundanten Nachrichten erzeugt. In einem weiteren Schritt d) wird eine 1-te Signatur der 1-ten gevoteten Nachricht durch das 1-te Votermodul mit einem 1-ten privaten Teilschlüssel erstellt, falls der 1-te Voter eine 1-te gevotete Nachricht erzeugt. In einem weiteren Schritt e) wird eine n-te Signatur und eine n-te gevoteten Nachricht von dem n-ten Votermodul an das (n+1)-te Votermodul übergeben. In einem weiteren Schritt f) wird die von dem (n+1)-ten Voter gevotete Nachricht mit der n-ten gevoteten Nachricht verglichen und eine (n+1)-te Signatur auf der n-ten Signatur mit einem (n+1)-ten privaten Teilschlüssel des (n+1)-ten Votermodul erstellt, falls die n-te gevotete Nachricht mit der (n+1)-ten gevoteten Nachricht übereinstimmt. In einem weiteren Schritt g) werden die Schritte e) und f) in aufsteigender Reihenfolge für jedes n mit $1 \leq n \leq (N-1)$ durchgeführt. In einem weiteren Schritt h) wird die N-te Signatur und die N-te gevotete Nachricht an eine Empfängereinheit übergeben. In einem weiteren Schritt i) wird die N-te gevotete Nachricht durch eine Empfängerkryptoeinheit akzeptiert, falls die Empfängerkryptoeinheit die N-te Signatur mit einem öffentlichen Schlüssel erfolgreich prüft.

Durch das erfindungsgemäße Verfahren wird das Prinzip des Votings mit kryptographischen Methoden kombiniert. Voraussetzung ist dabei immer, dass ein Voting einer Stufe erfolgreich ist und mit dem Votingresultat der Vorstufe übereinstimmt. Ohne diese Voraussetzung wird keine Teilsignatur durch einen Teilschlüssel erfolgen. Nur wenn aber alle Signaturen vorlie-

gen, dann „passt“ der öffentliche Schlüssel zu der durch die Teilschlüssel erzeugten Signatur und die gevotete Nachricht wird dann von der Empfängereinheit akzeptiert. Eine Empfängereinheit ist in anderen Worten eine Verifiziereinheit, ein
5 Verifiziergerät oder ein Empfänger. Durch das Konzept des verketteten Signierens wird eine hohe Sicherheit für die gevotete Nachricht erzeugt. Die Erfindung hat ferner den Vorteil, dass das Verfahren auf signaltechnisch nicht sicherer Hardware wie beispielsweise auf handelsüblichen PCs ausge-
10 führt werden kann.

Bevorzugt sind alle privaten Teilschlüssel voneinander verschieden.

15 Die Signaturen werden bevorzugt auf einem Hashwert der Nachricht gebildet. Dadurch wird das Datenvolumen von längeren Nachrichten vorteilhaft reduziert und der Prozess des verketteten Signierens kann schneller ablaufen.

20 Bevorzugt ergibt sich ein privater Schlüssel durch Multiplikation der privaten Teilschlüssel in der Restklasse und der öffentliche Schlüssel multipliziert mit dem sich ergebenden privaten Schlüssel ergibt in der Restklasse 1, wobei dadurch wieder der originale Hashwert oder die originale Nachricht
25 erhalten wird. Dies ist eine bevorzugte und besonders schnell ablaufende Realisierung der Signatur. Der originale Hashwert bzw. die originale Nachricht kann dann von der Empfängereinheit geprüft werden.

30 Bevorzugt ist der private Schlüssel kommutativ aus den privaten Teilschlüsseln berechenbar. Mit anderen Worten bedeutet das, dass es auf die Reihenfolge des Signierens nicht ankommt. Somit ist die Sequenz der verifizierenden Votermodule irrelevant, solange alle Votermodule beteiligt sind.

35

Vorteilhafterweise ist das Übergeben der gevoteten Nachricht des n-ten Votermoduls an das (n+1)-te Votermodul mit dem Übergeben der redundanten Nachrichten der Mehrzahl der

Replikanten (R_1, R_2, R_N) an das $(n+1)$ -te Votermodul zeitlich abgestimmt, wobei $1 \leq n \leq (N-1)$. Dadurch wird die zeitliche Verzögerung des verketteten Signierens verringert.

5 Bevorzugt ist jeder Voter von den anderen Votern separiert. Das meint, dass man die gleichen Techniken anwendet, wie man Replikanten segregiert, oder in anderen Worten kapselt bzw. isoliert. Dadurch wird die Unabhängigkeit der Berechnungspfade erreicht. Eine geeignete Kapselung der Votermodule kann
10 beispielsweise durch gefärbte Emulatoren für SIL3 oder SIL4 erzielt werden, wobei SIL das Sicherheits-Integritätslevel bezeichnet. Dies ist ferner von Vorteil, wenn man das Verfahren auf handelsüblichen PCs realisieren möchte.

15 Die Voter können als Diskriminatorvoter oder als Majoritätstvoter ausgeführt sein. Diskriminatorvoter geben eine gevotete Nachricht nur aus, falls alle Eingänge übereinstimmen. Majoritätstvoter bilden eine Mehrheitsentscheid, d.h. wenn eine Mehrheit der Nachrichten eine Übereinstimmung
20 aufweist, dann wird diese Nachricht ausgegeben

Ein Voter gibt bevorzugt keine Nachricht aus oder eine Negativnachricht, falls er keine gevotete Nachricht bilden kann.

25 Bevorzugt läuft das Übergeben der gevoteten Nachrichten vom n -ten Votermodul zum $(n+1)$ -ten Votermodul ohne Unterbrechung ab, wobei $1 \leq n \leq (N-1)$. Dadurch wird die Dauer des Signierens verringert.

30 Vorteilhafterweise kann jede redundante Nachricht des jeweiligen Replikanten sicherungstechnisch identifiziert werden. Dies kann beispielsweise durch eine Checksumme mit Replikantenidentifikation erfolgen.

35 Es wird ferner eine Vorrichtung zur Durchführung des Verfahrens zum Voting mit verketteten Signaturen vorgeschlagen. Die Vorrichtung umfasst eine Mehrzahl M von Replikanten zur Erzeugung von M redundanten Nachrichten mit $M \geq 2$. Ferner wird

eine Mehrzahl N von Votermodulen mit $N \geq 2$ bereitgestellt, wobei jedes Votermodul einen Voter zum Voting der redundanten Nachrichten sowie einen privaten Teilschlüssel zum Signieren einer Nachricht aufweist, wobei die Eingänge jedes Voters mit
5 den Ausgängen jedes Replikanten verbunden sind. Der Ausgang jedes n -ten Votermoduls ist mit dem Eingang jedes $(n+1)$ -ten Votermoduls zur Übertragung von gevoteten Nachrichten und Signaturen verbunden, wobei $1 \leq n \leq (N-1)$, und es ist eine Empfänger-
10 einheit vorgesehen, die die vom N -ten Votermodul ausgegebene Signatur und gevotete Nachricht empfängt und die N -te Signatur mit einem öffentlichen Schlüssel prüft.

Es wird ferner ein Computerprogramm vorgeschlagen, das es einer Datenverarbeitungseinrichtung ermöglicht, nachdem es in
15 Speichermittel der Datenverarbeitungseinrichtung geladen worden ist, ein Verfahren zum Voting mit verketteten Signaturen durchzuführen.

Ferner wird ein computerlesbares Speichermedium vorgeschlagen, auf dem ein Programm gespeichert ist, das es einer Datenverarbeitungseinrichtung ermöglicht, nachdem es in Spei-
20 chermittel der Datenverarbeitungseinrichtung geladen worden ist, ein Verfahren zum Voting mit verketteten Signaturen durchzuführen.

25 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. Es zeigen:

30

Figur 1 eine Darstellung des Verfahrens zum Voting mit verketteten Signaturen nach einer beispielhaften Ausführungs-
35 form, und

Figur 2 eine Darstellung einer Vorrichtung zum Voting mit verketteten Signaturen nach einer beispielhaften Ausführungsform.

5 In der Figur 1 ist ein Verfahren zum Voting mit verketteten Signaturen nach einer beispielhaften Ausführung gezeigt. Bereitgestellt sind jeweils eine Mehrzahl M von Replikanten R_1, R_2, R_M zur Erzeugung von M redundanten Nachrichten O_1, O_2, O_M , wobei $M \geq 2$. Diese redundanten Nachrichten O_1, O_2, O_M
10 sind inhaltlich äquivalent (von der Bedeutung her identisch). Zudem wird eine Mehrzahl N von Votermodulen VM_1, VM_2, VM_N bereitgestellt, wobei jedes Votermodul VM_1, VM_2, VM_N einen Voter V_1, V_2, V_N zum Voting der redundanten Nachrichten O_1, O_2, O_M sowie eine Kryptoeinheit K_1, K_2, K_N mit privatem Teilschlüssel
15 PR_1, PR_2, PR_N zum Signieren einer Nachricht aufweist.

Die redundanten Nachrichten O_1, O_2, O_M der Replikanten R_1, R_2, R_M werden an jedes Votermodul VM_1, VM_2, VM_3 übergeben, so dass der Voter V_1, V_2, V_N jedes Votermoduls VM_1, VM_2, VM_N eine gevotete
20 Nachricht auf Basis der redundanten Nachrichten erzeugt. In der Figur 1 ist das beispielhaft graphisch durch vertikale, gestrichelte Linien an jedem Votermodul VM_1, VM_2, VM_N angedeutet, auf die jeweils die redundanten Nachrichten O_1, O_2, O_M mittels dargestellter Pfeile zeigen.

25 Es wird dann eine 1-te Signatur der 1-ten gevoteten Nachricht M_1 durch das 1-te Votermodul VM_1 mit einem 1-ten privaten Teilschlüssel PR_1 erstellt, falls der 1-te Voter V_1 eine 1-te gevotete Nachricht M_1 erzeugt. Die 1-te Signatur wird hierbei
30 durch den Schlüsseloperator bzw. Schlüsselwert pri_1 des 1-ten privaten Teilschlüssels PR_1 angewendet auf die gevotete Nachricht M_1 oder alternativ auf einem Hashwert der Nachricht, was in der Figur mit $pri_1 \otimes M_1$ dargestellt wird. Diese 1-te Signatur wird dann mit der 1-ten gevoteten Nachricht M_1 an
35 das 2-te Votermodul VM_2 übergeben. In diesem 2-ten Votermodul VM_2 wird nun eine 2-te gevotete Nachricht M_2 durch den 2-ten Voter V_2 auf Basis der redundanten Nachrichten O_1, O_2, O_M der Replikanten R_1, R_2, R_M erstellt. Diese 2-te gevotete Nachricht

wird mit der 1-ten gevoteten Nachricht M1 verglichen. Bei Übereinstimmung wird dann eine 2-te Signatur mittels eines 2-ten privaten Teilschlüssel PR2 auf die 1-te Signatur erstellt, was durch $\text{pri}_2 \otimes \text{pri}_1 \otimes M1$ mit der Operation $\otimes$ dargestellt ist. Diese 2-te Signatur wird dann übergeben mit entweder der 1-ten gevoteten Nachricht M1 oder 2-ten gevoteten Nachricht M2. Da beide gevotete Nachrichten M1, M2 als Voraussetzung für das Signieren übereinstimmen müssen, ist es unerheblich, welche von beiden weitergeleitet wird. Das wird in der Figur 1 durch das ausschließende logische Kontravalenz-Symbol $\vee$ dargestellt, was einem „entweder oder“ entspricht. Beispielsweise kann die 1-te gevotete Nachricht M1 zum Übergeben verwendet werden.

Dieses Verfahren wird nun in dieser Form für die weiteren Votermodule VM1, VM2, VMN weitergeführt. Allgemeiner lässt sich daher formulieren, dass eine n-te Signatur und eine n-te gevotete Nachricht von dem n-ten Votermodul an das (n+1)-te Votermodul übergeben wird. Dann wird die von dem (n+1)-ten Voter gevotete Nachricht mit der n-ten gevoteten Nachricht verglichen und eine (n+1)-te Signatur auf der n-ten Signatur mit einem (n+1)-ten privaten Teilschlüssel des (n+1)-ten Votermoduls erstellt, falls die n-te gevotete Nachricht mit der (n+1)-ten gevoteten Nachricht übereinstimmt. Dies wird in aufsteigender Reihenfolge für jedes n mit $1 \leq n \leq (N-1)$ durchgeführt.

Im letzten Schritt wird somit eine N-te Signatur durch den N-ten privaten Teilschlüssel PRN auf die (N-1)-te Signatur erstellt, was in der Figur 1 durch $\text{pri}_N \otimes \dots \otimes \text{pri}_1 \otimes M1$ mit der Operation $\otimes$ dargestellt ist.

Danach wird die N-te Signatur und die N-te gevotete Nachricht MN (oder auch eine andere übereinstimmende gevotete Nachricht) an eine Empfängereinheit E übergeben. Dabei wird die N-te gevotete Nachricht MN durch eine Empfängerkryptoeinheit EK akzeptiert, falls die Empfängerkryptoeinheit EK die N-te

Signatur mit einem öffentlichen Schlüssel PU erfolgreich prüft.

Dieses Verfahren kann im Folgenden mathematisch beschrieben werden. Ein privater Schlüssel PR, im Folgenden mit pri bezeichnet, ergibt sich als Verknüpfung der privaten Teilschlüssel PR1, PR2, PRN, mit pri_n bezeichnet mit $1 \leq n \leq N$, mittels einer Operation $\otimes$, so dass $\text{pri}_N \otimes \dots \otimes \text{pri}_1 \equiv \text{pri} \pmod{a^l}$. Anders formuliert ist der private Schlüssel PR nicht prim, da er sich als Verknüpfung mehrerer Teilschlüssel P1, P2, PN darstellen lässt. Der private Schlüssel PR ergibt dann mit dem öffentlichen Schlüssel PU, hier als pub bezeichnet, durch Verknüpfung das neutrale Element 1 in der Restklasse, also $\text{pri} \otimes \text{pub} \equiv 1 \pmod{a^l}$, wobei a die Anzahl der möglichen Werte pro Zeichen, l die zu Grunde liegende Zeichenlänge, a^l die Anzahl der voneinander verschiedenen Schlüssel und $\equiv$ die Kongruenz repräsentiert. Der private Schlüssel PR und der öffentliche Schlüssel sind demnach modular invers zueinander bzgl. der Verknüpfung $\otimes$. Typischerweise arbeiten Prozessoren im binären System, was also $a=2$ entspricht und die bevorzugte Variante ist. Typischerweise liegt die Bitlänge l bei 128 bis 160 bit, jedoch können kürzere oder längere Bitlängen und somit kürzere und längere Schlüssel verwendet werden.

Wenn nun eine Signatur eines privaten Teilschlüssels Pr1, Pr2, PRN fehlen würde, dann würde es der Empfängereinheit E nicht gelingen die ursprüngliche Nachricht zurückzugewinnen. Durch das Konzept des verketteten Signierens wird eine hohe Sicherheit für die gevotete Nachricht erzeugt. Das Verfahren kann auf signaltechnisch nicht sicherer Hardware wie beispielsweise auf handelsüblichen PCs auszuführen. Durch das erfindungsgemäße Verfahren wird das Prinzip des Votings mit kryptographischen Methoden kombiniert. Voraussetzung ist dabei immer, dass ein Voting einer Stufe erfolgreich ist und mit dem Votingresultat der Vorstufe übereinstimmt. Ohne diese Voraussetzung wird keine Teilsignatur durch einen Teilschlüssel erfolgen. Nur wenn aber alle Signaturen vorliegen, dann „passt“ der öffentliche Schlüssel zu der durch die Teil-

schlüssel erzeugten Signatur und die Nachricht wird dann von der Empfängerseinheit E akzeptiert.

Als Verknüpfungen $\otimes$ kommen verschiedene zweckmäßigen Operationen in Frage. Beispielsweise sind auch Matrixverknüpfungen eingeschlossen. Dann ist beispielsweise die Reihenfolge der Signaturen wesentlich und kann im Allgemeinen nicht vertauscht werden. Alle privaten Teilschlüssel Pr_1, Pr_2, Pr_N sind ferner voneinander verschieden. Bevorzugt werden die Signaturen auf einem Hashwert der Nachricht gebildet. Dadurch wird das Datenvolumen von längeren Nachrichten vorteilhaft reduziert und der Prozess des verketteten Signierens kann schneller ablaufen.

Ein privater Schlüssel PR ergibt sich bevorzugt jedoch durch Multiplikation der privaten Teilschlüssel PR_1, PR_2, PR_N in der Restklasse. Der öffentliche Schlüssel PU multipliziert mit dem sich ergebenden privaten Schlüssel PR ergibt in der Restklasse 1, wobei dadurch wieder der originale Hashwert oder die originale Nachricht erhalten wird. Dies ist eine bevorzugte und besonders schnelle Realisierung der Signatur. Der originale Hashwert bzw. die originale Nachricht kann dann von der Empfängerseinheit E geprüft werden, beispielsweise indem mit der entsprechenden Hashfunktion aus der gevoteten Nachricht der Hashwert berechnet wird und mit dem übergebenen Hashwert nach Anwendung (Multiplikation) aller privaten Teilschlüssel verglichen wird.

Der private Schlüssel PR soll bevorzugt kommutativ aus den privaten Teilschlüsseln PR_1, PR_2, PR_N berechenbar sein. Dann ist die Sequenz der verifizierenden Votermodule VM_1, VM_2, VM_N irrelevant, solange zumindest alle Votermodule VM_1, VM_2, VM_N beteiligt sind. Dies ist beispielsweise bei der oben beschriebenen Multiplikation der Fall.

35

Es kann zusätzlich noch eine Synchronisation stattfinden. Sinnvoll für einen zügigen zeitlichen Ablauf des Signierens ist es, wenn das Übergeben der gevoteten Nachricht des n-ten

Votermoduls an das $(n+1)$ -te Votermodul mit dem Übergeben der redundanten Nachrichten $(O1, O2, OM)$ der Mehrzahl der Replikanten $(R1, R2, RN)$ an das $(n+1)$ -te Votermodul zeitlich abgestimmt wird, wobei $1 \leq n \leq (N-1)$. Dadurch wird die zeitliche
5 Verzögerung des verketteten Signierens verringert.

Jeder Voter $V1, V2, VN$ ist bevorzugt von den anderen Votern $V1, V2, VN$ separiert. Das meint, dass man hier die gleichen Techniken anwendet, wie man Replikanten $R1, R2, RM$ segregiert,
10 oder in anderen Worten kapselt bzw. isoliert. Dadurch wird die Unabhängigkeit der Berechnungspfade erreicht, wodurch das Risiko identischer Fehlerausgaben deutlich verringert wird. Eine geeignete Kapselung der Votermodule kann beispielsweise durch gefärbte Emulatoren für SIL3 oder SIL4 erzielt werden,
15 wobei SIL das Sicherheits-Integritätslevel bezeichnet. Dies ist ferner von Vorteil, wenn man das Verfahren auf handelsüblichen PCs realisieren möchte.

Die Voter $V1, V2, VN$ können als Diskriminatorvoter oder als
20 Majoritätsvoter ausgeführt werden. Diskriminatorvoter geben eine gevotete Nachricht nur aus, falls alle Eingänge übereinstimmen. Majoritätsvoter bilden eine Mehrheitsentscheid, d.h. wenn eine Mehrheit der Nachrichten eine Übereinstimmung aufweist, dann wird diese Nachricht ausgegeben. Ein Voter
25 $V1, V2, VN$ gibt bevorzugt keine Nachricht oder eine Negativnachricht aus, falls er keine gevotete Nachricht bilden kann. Dies wäre zum Beispiel dann der Fall, wenn beispielsweise ein Majoritätsvoter genau zwei Nachrichten erhält, die sich jedoch widersprechen. Im Falle eines Diskriminatorvoters wäre
30 das auch der Fall, wenn eine Eingangsnachricht von den Übrigen abweicht. Bevorzugt läuft das Übergeben der gevoteten Nachrichten vom n -ten Votermodul zum $(n+1)$ -ten Votermodul ohne Unterbrechung ab, wobei $1 \leq n \leq (N-1)$.

35 Vorteilhafterweise kann jede redundante Nachricht $O1, O2, OM$ des jeweiligen Replikanten $R1, R2, RM$ sicherungstechnisch identifiziert werden. Dies kann beispielsweise durch eine Checksumme mit Replikantenidentifikation erfolgen. Dadurch kann

beispielsweise das Fehlverhalten eines Replikanten R_1, R_2, R_M identifiziert werden.

In der Figur 2 wird beispielhaft eine Vorrichtung zum Voting mit verketteten Signaturen schematisch dargestellt. Dabei wird eine Mehrzahl M von Replikanten R_1, R_2, R_M zur Erzeugung von M redundanten Nachrichten mit $M \geq 2$ zur Verfügung gestellt. Zudem liegt eine Mehrzahl N von Votermodulen VM_1, VM_2, VM_N mit $N \geq 2$ vor. Dabei ist jedes Votermodul VM_1, VM_2, VM_N mit einem Voter V_1, V_2, V_N zum Voting der redundanten Nachrichten O_1, O_2, O_M der redundanten Replikanten R_1, R_2, R_M sowie einer Kryptoeinheit K_1, K_2, K_N mit einem privaten Teilschlüssel PR_1, PR_2, PR_N zum Signieren einer Nachricht ausgestattet, wobei die Eingänge jedes Votermoduls VM_1, VM_2, VM_N mit den Ausgängen jedes Replikanten R_1, R_2, R_N verbunden sind. Der Ausgang jedes n -ten Votermoduls ist mit dem Eingang jedes $(n+1)$ -ten Votermoduls zur Übertragung von gevoteten Nachrichten und Signaturen verbunden, wobei $1 \leq n \leq (N-1)$, und es ist eine Empfängereneinheit E vorgesehen, die die vom N -ten Votermodul VM_N ausgegebene Signatur und gevotete Nachricht empfängt und die N -te Signatur mit einem öffentlichen Schlüssel PU prüft.

Zusammengefasst wird ein Verfahren zum Voting vorgeschlagen, das mit (asymmetrischen) kryptographischen Methoden kombiniert wird. Dabei werden verkettete Signaturen in mehreren Stufen verwendet. Voraussetzung ist dabei immer, dass ein Voting einer Stufe erfolgreich ist und mit dem Votingresultat der Vorstufe übereinstimmt. Ohne diese Voraussetzung wird keine Teilsignatur durch einen Teilschlüssel erfolgen. Nur wenn aber alle Teilsignaturen vorliegen, dann „passt“ der öffentliche Schlüssel zu der durch die Teilschlüssel erzeugten Signatur und die Nachricht wird dann von der Empfängereneinheit E akzeptiert. Durch das Konzept des verketteten Signierens wird eine hohe Sicherheit für die gevotete Nachricht erzeugt. Dadurch kann das Verfahren auf signaltechnisch nicht sicherer Hardware wie beispielsweise auf handelsüblichen PCs ausgeführt werden.

Obwohl die Erfindung im Detail durch bevorzugte Ausführungsbeispiele näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzzumfang der Erfindung zu verlassen.

5

Bezugszeichenliste

	R1, R2, RM	Replikanten
	O1, O2, OM	redundante Nachrichten
5	VM1, VM2, VMN	Votermodul
	K1, K2, KN	Kryptoeinheit
	PR1, PR2, PRN	privater Teilschlüssel
	PR	privater Schlüssel
	E	Empfangseinheit
10	EK	Empfangskryptoeinheit
	PU	öffentlicher Schlüssel
	M1, M2, MN	gevote Nachricht

Patentansprüche

1. Verfahren zum Voting mit verketteten Signaturen umfassend die folgenden Schritte:

- 5 a) Bereitstellen einer Mehrzahl M von Replikanten (R_1, R_2, R_M) zur Erzeugung von M redundanten Nachrichten (O_1, O_2, O_M) mit $M \geq 2$;
- b) Bereitstellen einer Mehrzahl N von Votermodulen (VM_1, VM_2, VM_N) mit $N \geq 2$, wobei jedes Votermodul
10 (VM_1, VM_2, VM_N) einen Voter (V_1, V_2, V_N) zum Voting der redundanten Nachrichten sowie eine Kryptoeinheit (K_1, K_2, K_N) mit privatem Teilschlüssel (PR_1, PR_2, PR_N) zum Signieren einer Nachricht aufweist;
- c) Übergeben der redundanten Nachrichten (O_1, O_2, O_M) der
15 Replikanten (R_1, R_2, R_N) an jedes Votermodul (VM_1, VM_2, VM_N), so dass der Voter (V_1, V_2, V_N) jedes Votermoduls (VM_1, VM_2, VM_N) eine gevotete Nachricht (M_1, M_2, M_N) auf Basis der redundanten Nachrichten (O_1, O_2, O_M) erzeugt;
- 20 d) Erstellen einer 1-ten Signatur der 1-ten gevoteten Nachricht durch das 1-te Votermodul (VM_1) mit einem 1-ten privaten Teilschlüssel (PR_1), falls der 1-te Voter (V_1) eine 1-te gevotete Nachricht erzeugt;
- e) Übergeben einer n-ten Signatur und einer n-ten gevoteten
25 Nachricht von dem n-ten Votermodul an das (n+1)-te Votermodul;
- f) Vergleichen der von dem (n+1)-ten Voter gevoteten Nachricht mit der n-ten gevoteten Nachricht und Erstellen einer (n+1)-ten Signatur auf der n-ten Signatur mit ei-
30 nem (n+1)-ten privaten Teilschlüssel des (n+1)-ten Votermoduls, falls die 1-te gevotete Nachricht mit der (n+1)-ten gevoteten Nachricht übereinstimmt;
- g) Durchführen der Schritte e) und f) in aufsteigender Reihenfolge für jedes n mit $1 \leq n \leq (N-1)$;
- 35 h) Übergeben der N-ten Signatur und der N-ten gevoteten Nachricht an eine Empfängereinheit (E);
- i) Akzeptieren der N-ten gevoteten Nachricht durch eine Empfängerkryptoeinheit (EK), falls die

Empfängerkryptoeinheit (EK) die N-te Signatur mit einem öffentlichen Schlüssel (PU) erfolgreich prüft.

2. Verfahren nach Anspruch 1, wobei alle privaten Teilschlüssel (PR1, PR2, PRN) voneinander verschieden sind.
3. Verfahren nach einem der vorherigen Ansprüche, wobei die Signaturen auf einem Hashwert der Nachricht gebildet werden.
4. Verfahren nach einem der vorherigen Ansprüche, wobei sich ein privater Schlüssel (PR) durch Multiplikation der privaten Teilschlüssel (PR1, PR2, PRN) in der Restklasse ergibt und der öffentliche Schlüssel (PU) multipliziert mit dem sich ergebenden privaten Schlüssel (PR) in der Restklasse 1 ergibt, wobei dadurch wieder der originale Hashwert oder die originale Nachricht erhalten wird.
5. Verfahren nach einem der vorherigen Ansprüche, wobei ein privater Schlüssel (PR) kommutativ aus den privaten Teilschlüsseln (PR1, PR2, PRN) berechenbar ist.
6. Verfahren nach einem der vorherigen Ansprüche, wobei das Übergeben der gevoteten Nachricht des n-ten Votermoduls an das (n+1)-te Votermodul mit dem Übergeben der redundanten Nachrichten (O1, O2, OM) der Mehrzahl der Replikanten (R1, R2, RN) an das (n+1)-te Votermodul zeitlich abgestimmt wird, wobei $1 \leq n \leq (N-1)$.
7. Verfahren nach einem der vorherigen Ansprüche, wobei jeder Voter (V1, V2, VN) von den anderen Votern (V1, V2, VN) separiert wird.
8. Verfahren nach einem der vorherigen Ansprüche, wobei die Voter (V1, V2, VN) als Diskriminatorvoter oder als Majoritätstvoter ausgeführt werden.

9. Verfahren nach einem der vorherigen Ansprüche, wobei ein jeder Voter (V_1, V_2, V_N) keine Nachricht oder eine Negativnachricht erzeugt, falls er keine gevotete Nachricht bilden kann.

5 10. Verfahren nach einem der vorherigen Ansprüche, wobei das Übergeben der gevoteten Nachrichten vom n -ten Votermodul zum $(n+1)$ -ten Votermodul ohne Unterbrechung abläuft, wobei $1 \leq n \leq (N-1)$.

10 11. Verfahren nach einem der vorherigen Ansprüche, wobei bei jeder redundante Nachricht (O_1, O_2, O_N) der jeweilige Replikant (R_1, R_2, R_N) sicherungstechnisch identifiziert wird.

12. Vorrichtung zur Durchführung des Verfahrens zum Voting
15 mit verketteten Signaturen gemäß eines der Ansprüche 1-11:
- eine Mehrzahl M von Replikanten (R_1, R_2, R_N) zur Erzeugung von M redundanten Nachrichten mit $M \geq 2$;
- eine Mehrzahl N von Votermodulen (VM_1, VM_2, VM_N) mit $N \geq 2$, wobei jedes Votermodul (VM_1, VM_2, VM_N) einen Voter
20 (V_1, V_2, V_N) zum Voting der redundanten Nachrichten sowie einen privaten Teilschlüssel (PR_1, PR_2, PR_N) zum Signieren einer Nachricht aufweist, wobei die Eingänge jedes Voters (V_1, V_2, V_N) mit den Ausgängen jedes Replikanten (R_1, R_2, R_N) verbunden sind;
25 - der Ausgang jedes n -ten Votermoduls ist mit dem Eingang jedes $(n+1)$ -ten Votermoduls zur Übertragung von gevoteten Nachrichten und Signaturen verbunden, wobei $1 \leq n \leq (N-1)$, und es ist eine Empfängereinheit (E) vorgesehen, die die vom N -ten Votermodul (VM_N) ausgegebene Signatur und gevotete Nachricht empfängt und die N -te Signatur mit einem öffentlichen Schlüssel (PU) prüft.
30

13. Computerprogramm, das es einer Datenverarbeitungseinrichtung ermöglicht, nachdem es in Speichermittel der Datenverarbeitungseinrichtung geladen worden ist, ein Verfahren zum
35 Voting mit verketteten Signaturen gemäß eines der Ansprüche 1-11 durchzuführen.

14. Computerlesbares Speichermedium, auf dem ein Programm gespeichert ist, das es einer Datenverarbeitungseinrichtung ermöglicht, nachdem es in Speichermittel der Datenverarbeitungseinrichtung geladen worden ist, ein Verfahren zum Voting mit verketteten Signaturen gemäß eines der Ansprüche 1-11 durchzuführen.

FIG 1

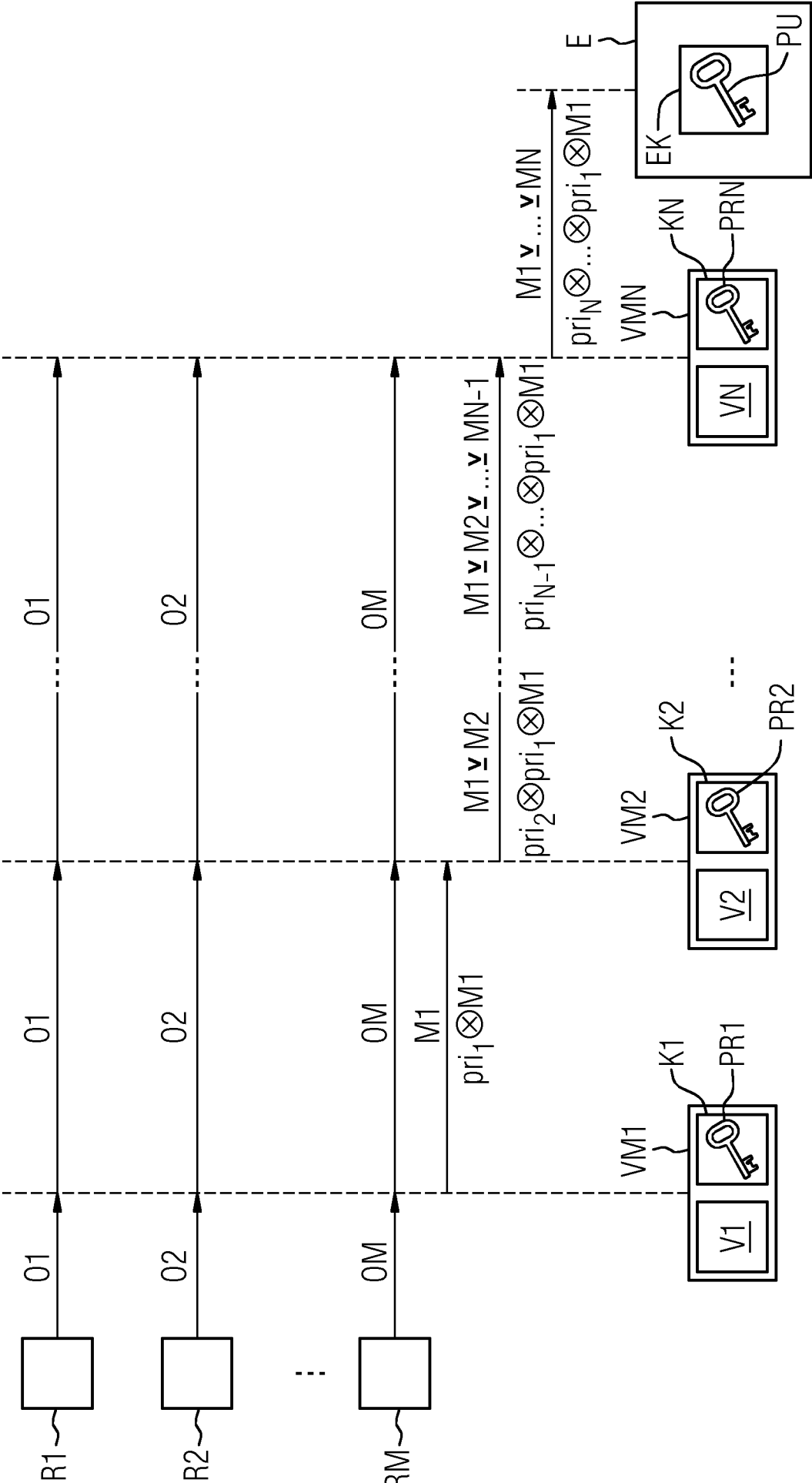
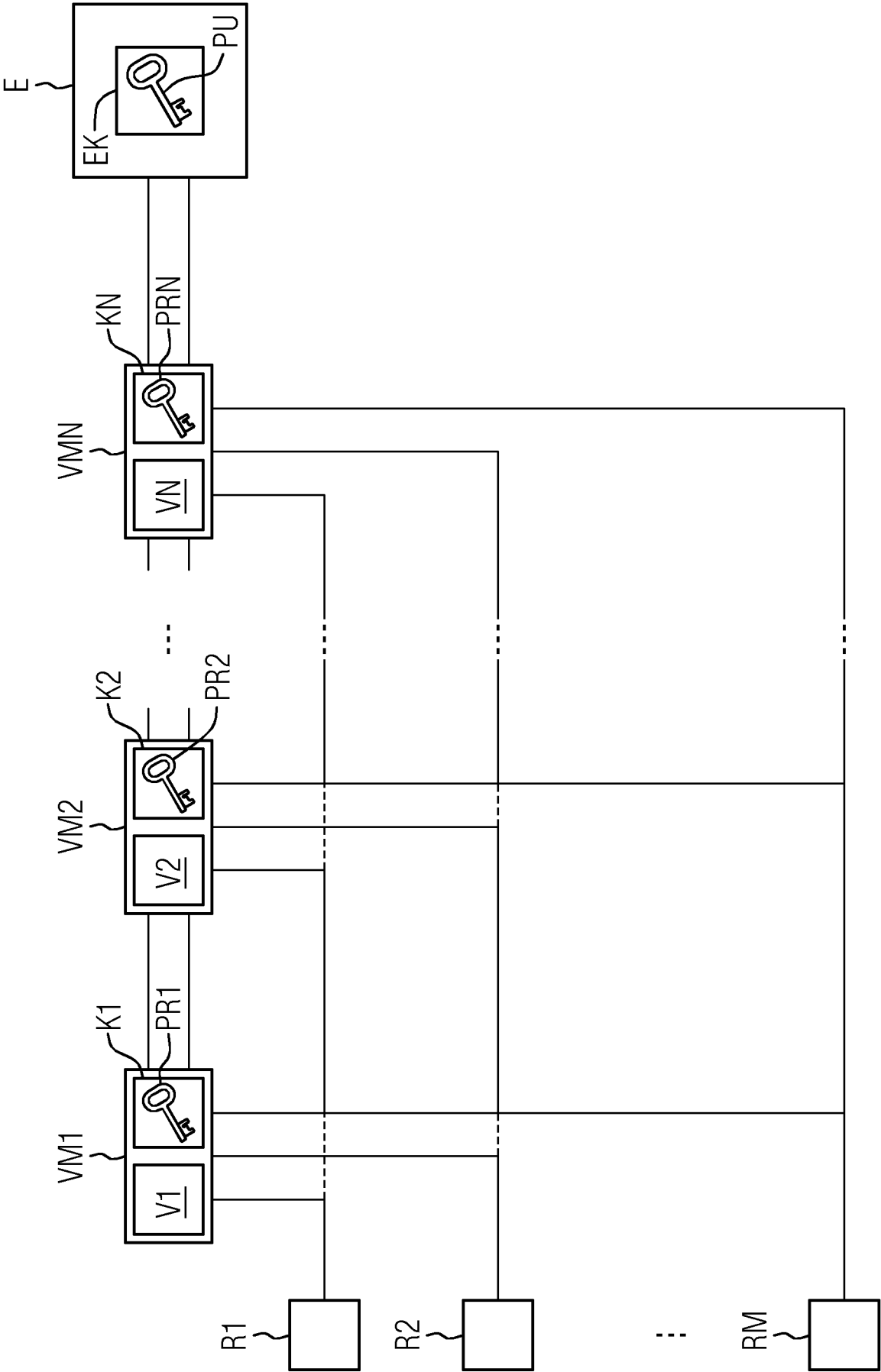


FIG 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/054745

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C13/00 H04L9/32
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)
G07C 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, INSPEC, 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	FR 2 926 911 A1 (RATIGNIER ALAIN THIERRY [FR]) 31 July 2009 (2009-07-31) abstract	1-14
A	DE 103 01 674 A1 (SIEMENS AG OESTERREICH [AT]) 13 November 2003 (2003-11-13) abstract; figure 2 column 1 - column 3	1-14
A	US 2013/191642 A1 (LOUGHRY ROBERT JOSEPH [US]) 25 July 2013 (2013-07-25) abstract	1-14
A	WO 01/73694 A2 (VOTEHERE INC [US]; NEFF C ANDREW [US]) 4 October 2001 (2001-10-04) abstract page 1 - page 4	1-14



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

4 May 2017

Date of mailing of the international search report

16/05/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/054745

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2926911	A1	31-07-2009	NONE
DE 10301674	A1	13-11-2003	CH 696783 A5 30-11-2007 DE 10301674 A1 13-11-2003
US 2013191642	A1	25-07-2013	NONE
WO 0173694	A2	04-10-2001	AT 309655 T 15-11-2005 AU 5097601 A 08-10-2001 CA 2404161 A1 04-10-2001 DE 60114833 D1 15-12-2005 DE 60114833 T2 13-04-2006 DK 1302020 T3 20-03-2006 EP 1302020 A2 16-04-2003 ES 2251475 T3 01-05-2006 JP 2003529256 A 30-09-2003 JP 2006115550 A 27-04-2006 US 2002007457 A1 17-01-2002 WO 0173694 A2 04-10-2001

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. G07C13/00 H04L9/32
 ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 G07C 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, INSPEC, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FR 2 926 911 A1 (RATIGNIER ALAIN THIERRY [FR]) 31. Juli 2009 (2009-07-31) Zusammenfassung -----	1-14
A	DE 103 01 674 A1 (SIEMENS AG OESTERREICH [AT]) 13. November 2003 (2003-11-13) Zusammenfassung; Abbildung 2 Spalte 1 - Spalte 3 -----	1-14
A	US 2013/191642 A1 (LOUGHRY ROBERT JOSEPH [US]) 25. Juli 2013 (2013-07-25) Zusammenfassung -----	1-14
A	WO 01/73694 A2 (VOTEHERE INC [US]; NEFF C ANDREW [US]) 4. Oktober 2001 (2001-10-04) Zusammenfassung Seite 1 - Seite 4 -----	1-14



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

4. Mai 2017

Absendedatum des internationalen Recherchenberichts

16/05/2017

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

San Millán Maeso, J

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2017/054745

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2926911	A1	31-07-2009	KEINE
DE 10301674	A1	13-11-2003	CH 696783 A5 30-11-2007 DE 10301674 A1 13-11-2003
US 2013191642	A1	25-07-2013	KEINE
WO 0173694	A2	04-10-2001	AT 309655 T 15-11-2005 AU 5097601 A 08-10-2001 CA 2404161 A1 04-10-2001 DE 60114833 D1 15-12-2005 DE 60114833 T2 13-04-2006 DK 1302020 T3 20-03-2006 EP 1302020 A2 16-04-2003 ES 2251475 T3 01-05-2006 JP 2003529256 A 30-09-2003 JP 2006115550 A 27-04-2006 US 2002007457 A1 17-01-2002 WO 0173694 A2 04-10-2001