(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
19. Mai 2005 (19.05.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/046157 A3

(51) Internationale Patentklassifikation[7]: H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP2004/052909

(22) Internationales Anmeldedatum:
10. November 2004 (10.11.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 52 538.6 11. November 2003 (11.11.2003) DE
103 58 987.2 16. Dezember 2003 (16.12.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HORN, Günther** [DE/DE]; Eduard-Schmid-Str. 16, 81541 München (DE).

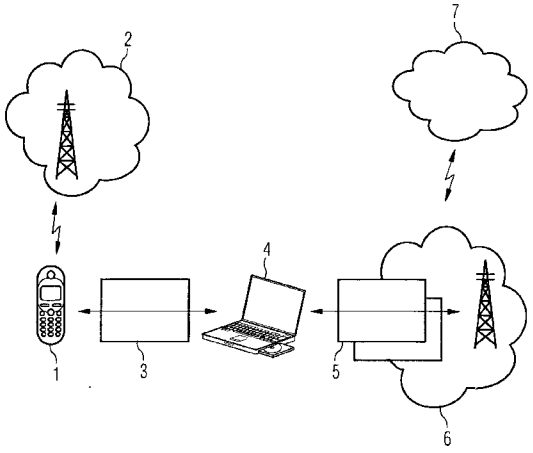
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR SAFEGUARDING DATA TRANSMISSION BETWEEN A FIRST TERMINAL AND A FIRST NETWORK AND BETWEEN A SECOND TERMINAL AND A SECOND NETWORK

(54) **Bezeichnung:** VERFAHREN ZUR SICHERUNG DES DATENVERKEHRS ZWISCHEN EINEM ERSTEN ENDGERÄT UND EINEM ERSTEN NETZ SOWIE EINEM ZWEITEN ENDGERÄT UND EINEM ZWEITEN NETZ



(57) **Abstract:** The invention relates to a method for safeguarding data transmission between a first terminal (1) and a first network (2) and between a second terminal (4) and a second network (6), wherein the first terminal (1) can communicate in the first network (2) with the aid of one or several session keys and the second terminal (4) can communicate in the second network (6) with the aid of one or several session keys. The inventive method is characterised in that the first terminal (1) is connected to the second terminal (4) through a local interface (3); in the first terminal (1), one or several first session keys are determined and one or several second session keys are derived from said first session keys; one or several second session keys are transmitted to the second terminal (4) through said local interface by means of a safety protocol; the second terminal (4) is authenticated to the second network (6) by means of one or several second session keys and/ or by means of the key derived from the second session keys through an authentication protocol.

[Fortsetzung auf der nächsten Seite]

WO 2005/046157 A3

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 7. Juli 2005

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Sicherung des Datenverkehrs zwischen einem ersten Endgerät (1) und einem ersten Netz (2) sowie einem zweiten Endgerät (4) und einem zweiten Netz (6), wobei das erste Endgerät (1) mithilfe eines oder mehrerer erster Sitzungsschlüssel in einem ersten Netz (2) kommunizieren kann und das zweite Endgerät (4) mithilfe eines oder mehrerer zweiter Sitzungsschlüssel in einem zweiten Netz (6) kommunizieren kann, gekennzeichnet durch folgende Schritte: das erste Endgerät (1) wird mit dem zweiten Endgerät (4) über eine lokale Schnittstelle (3) verbunden; im ersten Endgerät (1) werden der oder die ersten Sitzungsschlüssel ermittelt und der oder die zweiten Sitzungsschlüssel aus den ersten Sitzungsschlüsseln abgeleitet; der oder die zweiten Sitzungsschlüssel werden über die lokale Schnittstelle (3) mittels eines Sicherheitsprotokolls das zweite Endgerät (4) wird mithilfe des oder der zweiten Sitzungsschlüssel und/oder mithilfe aus dem oder den zweiten Sitzungsschlüsseln abgeleiteter Schlüssel über ein Authentifikationsprotokoll an dem zweiten Netz (6) authentifiziert.