(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
26. April 2007 (26.04.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/045395 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2006/009861

(22) Internationales Anmeldedatum:
11. Oktober 2006 (11.10.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
05022902.0 20. Oktober 2005 (20.10.2005) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **UBS AG** [CH/CH]; Bahnhofstrasse 45, CH-8001 Zürich (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HILTGEN, Alain P.** [CH/CH]; Viktoriastrasse 23, CH-8057 Zürich (CH).

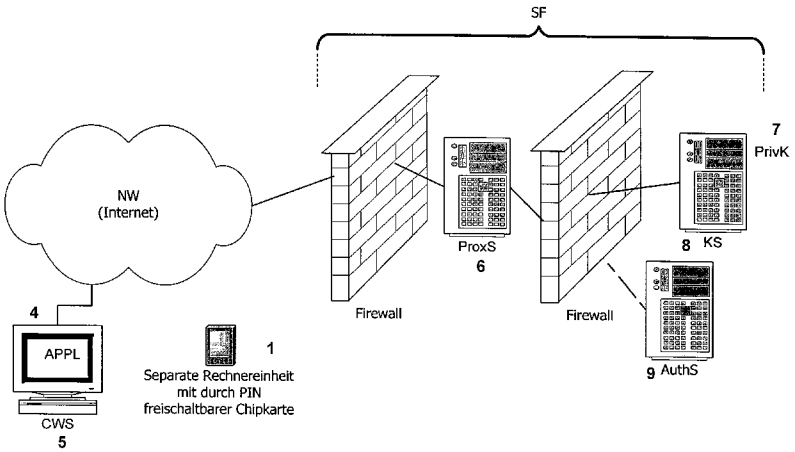
(74) Anwalt: **SCHMIDT, Steffen, J.**; WUESTHOFF & WUESTHOFF, Schweigerstrasse 2, 81541 München (DE).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

(54) **Title:** DEVICE AND METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS IN A SERVER-CLIENT COMPUTER NETWORK SYSTEM

(54) **Bezeichnung:** VORRICHTUNGEN UND VERFAHREN ZUM DURCHFÜHREN VON KRYPTOGRAPHISCHEN OPERATIONEN IN EINEM SERVER-CLIENT-RECHNERNETZWERKSYSTEM



1 ... INDIVIDUAL COMPUTER UNIT PROVIDED WITH A FREELY SWITCHABLE CHIP CARTE BY MEANS OF A PIN
4 ... APPLICATION
5 ... CLIENT COMPUTER WORKSTATION
6 ... PROXY SERVER
7 ... PRIVATE KEY
8 ... CRYPTOGRAPHY SERVER COMPUTER SYSTEM
9 ... AUTHENTICATION SERVER

(57) **Abstract:** In a server-client computer network system for carrying out cryptographic operations between a client computer workstation and a cryptography server computer system, a computer software programs for communication therebetween are installed in the client computer workstation and in the cryptography server computer system. Said computer software programs are executed in such a way that, when the client computer workstation transmits a request for carrying out a cryptographic operation to the cryptography server computer system, said computer workstation receives an answer therefrom. For this purpose, the cryptography server computer system requests a strong authentication from the client computer workstation. In response, the client computer workstation engages the key of the user thereof for producing said strong authentication. In the case of the successful authentication, the client computer workstation receives a release for initiating one or several cryptographic operations with the aid of the private key. According to said invention, the privet key is stored in the cryptography server computer system and cryptographic operation(s) is (are) authorised for a fixed short time after the successful authentication for carrying out the cryptographic operation(s) requested by the computer software program operating on the client computer workstation. At the same time, the client computer workstation puts at the disposal of the application software program the result of the cryptographic operation(s).

[Fortsetzung auf der nächsten Seite]

WO 2007/045395 A1

(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, LT, LU, LV, 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).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

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: In einem Server-Client-Rechnernetzwerksystem sind zum Durchführen von kryptografischen Operationen über ein Netzwerk zwischen einer Client-Rechner-Arbeitsstation und einem Kryptografie-Server-Rechnersystem, in der Client-Rechner-Arbeitsstation und in dem Kryptografie-Server-Rechnersystem zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert. Diese Computersoftware-Programme werden ausgeführt, damit, wenn die Client-Rechner-Arbeitsstation eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem richtet, diese von dem Kryptografie-Server-Rechnersystem beantwortet wird. Dazu fordert das Kryptografie-Server-Rechnersystem von der anfragenden Client-Rechner-Arbeitsstation eine starke Authentifizierung an. Als Reaktion hierauf greift die Client-Rechner-Arbeitsstation unter einer starken Authentifizierung auf einen Schlüssel ihres Nutzers zu. Bei erfolgreicher Authentifizierung erhält die Client-Rechner-Arbeitsstation eine Freigabe dafür, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel zu initiieren. Dabei ist erfindungsgemäß der private Schlüssel auf dem Kryptografie-Server-Rechnersystem abgelegt, und die kryptografische/n Operation/en wird/werden nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen, um die von einer auf der Client-Rechner-Arbeitsstation ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en auszuführen. Dabei stellt die Client-Rechner-Arbeitsstation das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung.