(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
8. August 2013 (08.08.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/113050 A1

(51) Internationale Patentklassifikation:
H04L 9/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/AT2013/000013

(22) Internationales Anmeldedatum:
28. Januar 2013 (28.01.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 131/2012 31. Januar 2012 (31.01.2012) AT

(71) Anmelder: **FINALOGIC BUSINESS TECHNOLOGIES GMBH** [AT/AT]; Kärntner Ring 5-7, 7. Stock - Regus Office, A-1010 Wien (AT).

(72) Erfinder: **BEIDL, Heinrich**; Kleistgasse 22/7, A-1030 Wien (AT). **HRDY, Erwin**; Brahmsgasse 7, Haus 1, A-2232 Deutsch-Wagram (AT). **SCHAUERHUBER, Julius**; Pfarrgasse 13, A-3462 Absdorf (AT).

(74) Anwälte: **HOLZER, Walter** et al.; Schütz u. Partner, Brigittenauer Lände 50, A-1200 Wien (AT).

(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).

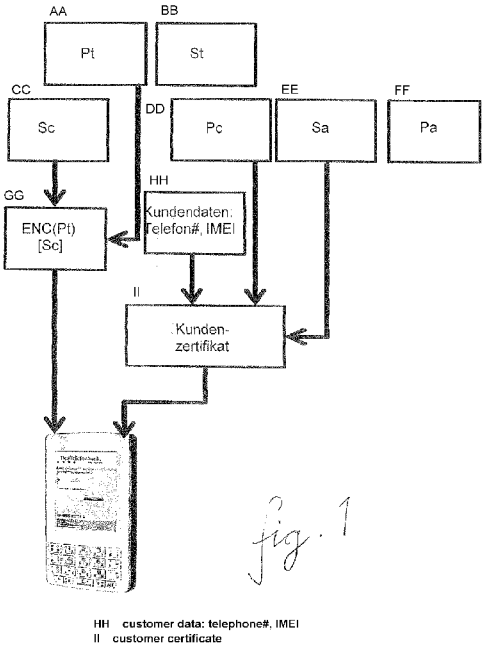
Veröffentlicht:

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

WO 2013/113050 A1

(54) **Title**: CRYPTOGRAPHIC AUTHENTICATION AND IDENTIFICATION METHOD USING REAL-TIME ENCRYPTION

(54) **Bezeichnung** : KRYPTOGRAPHISCHES AUTHENTIFIZIERUNGS - UND IDENTIFIKATIONSVERFAHREN MIT REALZEITVERSCHLÜSSELUNG



(57) **Abstract**: The invention relates to a method for securing data and safeguarding the data origin, said data being transmitted from a customer device to a center in an electronically encrypted manner. The method has the following steps: • i) generating and storing an RSA key pair consisting of a first key (Sa) and a second key (Pa) for signing customer certificates in the center, • ii) generating and storing two RSA key pairs for the customer device, said key pairs consisting of a third key of the customer device (Sc) and a fourth key of the customer device (Pc) as well as a first key encryption key (St) and a second key encryption key (Pt), • iii) generating an encrypted key by encrypting the third key of the customer device (Sc) using the second key encryption key (Pt) and generating a customer certificate in the center, • iv) transmitting the encrypted key and the customer certificate to the customer device, • v) transmitting the first key encryption key (St) to the customer device in response to a request by the customer device, • vi) decrypting the encrypted key using the first key encryption key (St) in the customer device, the third key of the customer device (Sc) being obtained, • vii) encrypting a randomized sequence of numbers in the center using the fourth key of the customer device (Pc), • viii) transmitting the encrypted randomized sequence of numbers, • ix) decrypting the encrypted randomized sequence of numbers in the customer device, • x) encrypting a first PIN entry on the customer device into a ciphertext using the third key of the customer device (Sc), • xi) transmitting the ciphertext and the customer certificate to the center, and • xii) decrypting the ciphertext in the center using the fourth key of the customer device (Pc) and decrypting the first PIN entry.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

Verfahren zur Sicherung von Daten und Sicherstellung ihres Ursprungs, wobei die Daten von einem Kundengerät an eine Zentrale elektronisch verschlüsselt übermittelt werden, und wobei das Verfahren die folgenden Schritte umfaßt: • i) Erzeugen und Speichern eines RSA-Schlüsselpaares bestehend aus einem ersten Schlüssel (Sa) und einem zweiten Schlüssel (Pa) für das Signieren von Kundenzertifikaten in der Zentrale, • ii) Generieren und Speichern zweier RSA-Schlüsselpaare für das Kundengerät bestehend aus einem dritten Schlüssel des Kundengerätes (Sc) und einem vierten Schlüssel des Kundengerätes (Pc) sowie einem ersten Schlüsselverschlüsselungsschlüssel (St) und einem zweiten Schlüsselverschlüsselungsschlüssel (Pt), •iii) Erzeugen eines verschlüsselten Schlüssels durch Verschlüsseln des dritten Schlüssels des Kundengerätes (Sc) mit dem zweiten Schlüsselverschlüsselungsschlüssel (Pt) sowie Generieren eines Kundenzertifikats in der Zentrale, •iv) Übermitteln des verschlüsselten Schlüssels und des Kundenzertifikats an das Kundengerät, • v) Senden des ersten Schlüsselverschlüsselungsschlüssels (St) an das Kundengerät nach einer Anforderung durch das Kundengerät, •vi) Entschlüsseln des verschlüsselten Schlüssels mit dem ersten Schlüsselverschlüsselungsschlüssel (St) in dem Kundengerät, wobei der dritte Schlüssel des Kundengerätes (Sc) erhalten wird, •vii) Verschlüsseln einer verreihten Ziffernanordnung in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc), • viii) Senden der verschlüsselten verreihten Ziffernanordnung ix) Entschlüsseln der verschlüsselten verreihten Ziffernanordnung im Kundengerät •x) Verschlüsseln einer ersten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat, • xi) Senden des Chiffrats und des Kundenzertifikats an die Zentrale, • xii) Entschlüsseln des Chiffrats in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc), Entschlüsseln der ersten PIN-Eingabe

KRYPTOGRAPHISCHES AUTHENTIFIZIERUNGS - UND IDENTIFIKATIONSVERFAHREN MIT REALZEITVERSCHLÜSSELUNG

Die Erfindung betrifft ein Verfahren zur Sicherung von Daten und Sicherstellung ihres Ursprunges, wobei die Daten von einem Kundengerät an eine Zentrale elektronisch verschlüsselt übermittelt werden.

Im Stand der Technik sind Verfahren zur sicheren Übermittlung elektronischer Daten mit Hilfe von digitalen Verschlüsselungstechniken bekannt.

Die US 2002 059 146 A1 zeigt ein Verfahren zur Identifizierung eines Anwenders und zur sicheren Übermittlung von Zahlencodes. Dabei wird ein Transactionscode durch Verschlüsselung einer zufälligen Zahl mit der PIN des Anwenders, welche nur dem Anwender und einer Zentrale bekannt ist, verwendet. Nachteilig ist hier, daß bereits das Ausspähen der PIN die Sicherheit dieses Verfahrens gefährdet.

Die AT 504 634 B1 sowie die WO 2008 151 209 A1, auch veröffentlicht als US 2008 298 588 A1, offenbaren Verfahren zum Transferieren von verschlüsselten Nachrichten. Dabei wird unter wechselnder Verwendung von symmetrischen und asymmetrischen Schlüsseln, wie etwa RSA-Schlüsselpaaren, eine Nachricht über einen dritten Kommunikationspunkt, die sogenannte Authentifikationseinrichtung, gesendet, die erst bei erfolgreicher gegenseitiger Identifizierung des Senders und Empfängers sowie entsprechender Übermittlung von Schlüsseln untereinander die Nachrichtenübertragung freigibt. Nachteil dieser Lehre ist, daß permanent ein dritter Kommunikationspunkt, beispielsweise in Form eines Servers, betrieben werden muß.

Die WO 2008 076 442 A1 lehrt ein Verfahren zur Verreihung der Nummern auf einem Nummernfeld, auf welchem beispielsweise eine

PIN eingegeben wird. Das mechanische Nummernfeld bleibt unverändert, jedoch ignoriert der Anwender bei der Eingabe die (standardisierte) Ziffernbeschriftung der Tasten. Ihm wird über eine Bildschirmanzeige eine neue Verteilung der Ziffern 0 bis 9 vorgegeben, wonach er seine PIN in das Nummernfeld eingibt. Dadurch ist das Ausspähen der PIN durch Dritte erschwert. Nachteilig ist, daß diese Sicherheitsmaßnahme wirkungslos ist, wenn ausspähende Dritte auch den Algorithmus zur Verreihung der Nummern kennen.

Die US 2003 182 558 A1 zeigt ebenfalls ein Verfahren zur Verreihung von Ziffern eines Nummernfeldes, wobei die Ziffern zusätzlich in einer anderen Geometrie als der herkömmlichen Tastaturanordnung auf einem berührungsempfindlichen Bildschirm dargestellt werden. Der Nachteil des wirkungslosen Schutzes bei Kenntnis des Darstellungsalgorithmus bleibt jedoch.

Es ist die Aufgabe des erfindungsgemäßen Verfahrens, die Nachteile im Stand der Technik zu überwinden und ein Verfahren anzugeben, bei welchem es nicht möglich ist, durch Ausspähen einer Nummerneingabe oder Kenntnis eines oder mehrerer Schlüssel bei der Übermittlung von Daten die Identität des Absenders und den Inhalt der Daten zu verändern.

Laut dem Prinzip von Kerkhoff von 1883 ist ein Kryptosystem sicher, trotzdessen ein Angreifer alle Systemdetails kennt, solange die Schlüssel geheim bleiben (Kerkhoff's Principle [1883]: A cryptosystem should be secure even if the attacker knows all the details about the system, with the exception of the secret key).

Die Aufgaben werden erfindungsgemäß dadurch erreicht, daß das Verfahren die folgenden Schritte umfaßt:

i) Erzeugen und Speichern eines RSA-Schlüsselpaares bestehend aus einem ersten Schlüssel (Sa) und einem zweiten

Schlüssel (Pa) für das Signieren von Kundenzertifikaten in der Zentrale,

ii) Generieren und Speichern zweier RSA-Schlüsselpaare für das Kundengerät bestehend aus einem dritten Schlüssel des Kundengerätes (Sc) und einem vierten Schlüssel des Kundengerätes (Pc) sowie einem ersten Schlüsselverschlüsselungsschlüssel (St) und einem zweiten Schlüsselverschlüsselungsschlüssel (Pt), wobei der erste Schlüsselverschlüsselungsschlüssel (St) und der zweite Schlüsselverschlüsselungsschlüssel (Pt) zum gesicherten Transport des dritten Schlüssels des Kundengerätes (Sc) geeignet sind,

iii) Erzeugen eines verschlüsselten Schlüssels durch Verschlüsseln des dritten Schlüssels des Kundengerätes (Sc) mit dem zweiten Schlüsselverschlüsselungsschlüssel (Pt) sowie Generieren eines Kundenzertifikats in der Zentrale durch Verschlüsseln der kundenspezifischen Telefonnummer sowie der IMEI des Kundengerätes und/oder einer Kundennummer mit dem vierten Schlüssel des Kundengerätes (Pc) und anschließendem Verschlüsseln mit dem ersten Schlüssel (Sa) für das Signieren von Kundenzertifikaten,

iv) Übermitteln des verschlüsselten Schlüssels und des Kundenzertifikats an das Kundengerät,

v) Senden des ersten Schlüsselverschlüsselungsschlüssels (St) an das Kundengerät nach einer Anforderung durch das Kundengerät,

vi) Entschlüsseln des verschlüsselten Schlüssels mit dem ersten Schlüsselverschlüsselungsschlüssel (St) in dem Kundengerät, wobei der dritte Schlüssel des Kundengerätes (Sc) erhalten wird,

vii) Verschlüsseln einer verreihten Ziffernanordnung in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc),

viii) Senden der verschlüsselten verreihten Ziffernanordnung an das Kundengerät,

ix) Entschlüsseln der verschlüsselten verreihten Ziffernanordnung im Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc),

x) Verschlüsseln einer ersten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat,

xi) Senden des Chiffrats und des Kundenzertifikats an die Zentrale,

xii) Entschlüsseln des Chiffrats in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc), Entschlüsseln der ersten PIN-Eingabe und Überprüfen des zugesendeten Kundenzertifikats mit dem in der Zentrale gespeicherten Kundenzertifikat.

Bevorzugt ist in einer Ausgestaltung der Erfindung, daß das Chiffrat in der Zentrale entschlüsselt und daß das vom Kundengerät übermittelte Zertifikat mit dem in der Zentrale gespeicherten Zertifikat verglichen wird, um die Authentizität der Daten zu verifizieren.

Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens, daß die Verreihung der verreihten Ziffernanordnung bei der Initialisierung des Verfahrens einmalig vom Kunden gewählt und an die Zentrale übermittelt wird.

Bevorzugt ist in einer Ausgestaltung der Erfindung, daß die Verreihung der verreihten Ziffernanordnung in der Zentrale für jede Übermittlung an das Kundengerät neu generiert wird.

Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens, daß das Verfahren die weiteren Schritte umfaßt:

iii.a) Generieren eines Zeitstempels in der Zentrale,

iv.a) Übermitteln des verschlüsselten Schlüssels zusammen mit dem Zeitstempel an das Kundengerät,

x.a) Verschlüsseln der ersten PIN-Eingabe am Kundengerät zusammen mit dem Zeitschlüssel zu einem Chiffrat.

Eine bevorzugte Ausführungsform des Verfahrens zeichnet sich durch die weiteren Schritte aus:

x.b) Verschlüsseln einer zweiten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat, um eine neue PIN zur Zentrale zu schikken, und

x.c) Verschlüsseln einer dritten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat, um die neue PIN zu bestätigen.

Bevorzugt ist in einer Ausgestaltung der Erfindung, daß zusätzlich zur ersten PIN-Eingabe die Nummerneingabe einer Kreditkartennummer und/oder ein Ablaufdatum einer Kreditkarte und/oder eine Prüfziffer einer Kreditkarte erfolgt und zusammen mit der ersten PIN-Eingabe verschlüsselt an die Zentrale übermittelt wird.

Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens, daß zusätzlich zur ersten PIN-Eingabe die Nummerneingabe einer warenspezifischen Zahl, wie z.B. die ISBN eines Buchtitels, erfolgt und zusammen mit der ersten PIN-Eingabe verschlüsselt an die Zentrale übermittelt wird.

Die Erfindung wird nachstehend anhand eines in den Zeichnungen dargestellten Ausführungsbeispiels näher erläutert. Es zeigen: Fig. 1 eine schematische Darstellung der Übermittlung vorbereitender Daten an ein Kundengerät, Fig. 2 ein schematisches Kundengerät, und die Fig. 3a bis 3d verschieden verreihte Ziffernanordnungen auf einem Nummernfeld.

Das Verfahren, das auch als Finalogic-System bezeichnet wird, wird von Inhabern von beispielsweise mobilen Telefon- und Kommunikationsgeräten benutzt, um auf gesicherten Prozessen Rechtsgeschäfte ausführen zu können. Das sind etwa die Bestellung von Waren oder Dienstleistungen sowie der Zugriff auf geschützte Informationen.

Dies betrifft folglich den Schutz von numerischen und/oder auch alphanumerischen Dateneingaben an mobilen Telefon- und Kommunikationsgeräte vor Kenntnisnahme unberechtigter Dritter.

Solche Dateneingaben können sein und werden in dem Verfahren angewendet bei der

- Festlegung, Eingabe und Änderung der PIN des Mobiltelefonhalters und der
- Eingabe von Kreditkartendaten des Mobiltelefon- bzw. Kommunikationsgerätehalters.

Dies betrifft ebenso Verfahrensschritte für die Überprüfung der Echtheit des Ursprungs und Inhalt von funktechnisch übermittelten Daten von mobilen Telefon- und Kommunikationsgeräten, die Identität des Absenders und die Verhinderung der

freien Lesbarkeit sensitiver Informationen durch unberechtigte Dritte unter Verwendung kryptographischer Methoden in Realzeitverschlüsselung zur Aktionsperiode.

Zur Nutzung des erfindungsgemäßen Verfahrens muß sich der Kunde, das ist ein Inhaber eines mobilen Telefon- und Kommunikationsgerätes, im folgenden auch Kundengerät, entweder telefonisch oder via einer Internetseite, wie etwa Finalogics Webseite, registrieren lassen.

Dabei wird er - neben den erforderlichen persönlichen Daten - auch um die Type seines Gerätes gefragt, beispielsweise iPhone4. Des weiteren kann es Wunsch des Kunden sein, schon zu diesem Zeitpunkt zum Beispiel die Art seiner Bezahlweise, beispielsweise Kreditkarte oder die Berechtigungspaßwörter für den Zugang zu bestimmten Informationsservices, anzugeben. Wichtig ist, daß die eigentlichen Zugangsdaten, welche besonders sensitiven Informationscharakter haben, erst zu einem späteren Zeitpunkt im System bekanntgegeben werden müssen.

Abschließend wird der Kunde noch um zwei Datenelemente seines Geräts gefragt:

i. die eigene Telefonnummer (Phone#) und

ii. die 15-stellige IMEI - International Mobile Equipment Identifier, Hardwareidentifikationsnummer - sie ist weltweit einmalig für jedes mobile Telefon- oder Kommunikationsgerät. Diese Nummer kann jeder Kunde selbst durch die Tastenkombination *#06# aus seinem Gerät auslesen.

Alternativ oder zusätzlich zur IMEI, die nicht sehr gut zu schützen und in manchen Fällen auch mehrfach an viele Geräte vergeben wird, kann zwischen Kunde und Zentrale eine Kundennummer vereinbart werden. Im folgenden wird dann die Verwendung dieser Kundennummer anstatt oder zusammen mit der IMEI

die Sicherheit des erfindungsgemäßen Verfahrens zusätzlich steigern.

Nach Eingabe dieser Informationen in das Finalogic-System ist der Registrierungsprozess beendet.

Nun beginnt der Kryptographische Initialisierungsprozeß zur Sicherstellung der Echtheit des Ursprunges und zur Echtheit von elektronisch übermittelten Daten oder auch das Verfahren zur Sicherung von Daten und Sicherstellung ihres Ursprungs. Dabei arbeitet das Finalogic-System mit Datenelementen der PKI - Public Key Infrastructure, gemäß dem internationalen Standard IEEE P1363.

Es werden asymmetrische Schlüsselpaare verwendet, die aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) bestehen. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Authentifikation ist dabei die Identifikation der eigenen Person. Der private Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren.

Folgende asymmetrische Schlüsselpaare finden Verwendung:

i. ein erster Schlüssel für das Signieren von Kundenzertifikaten Sa, der sogenannte geheime PrivateKey(Finalogic);

ii. ein zweiter Schlüssel Pa für das Signieren von Kundenzertifikaten, der sogenannte öffentliche PublicKey(Finalogic);

iii. ein erster Schlüsselverschlüsselungsschlüssel St, der sogenannte geheime PrivateKey(Trans);

iv. ein zweiter Schlüsselverschlüsselungsschlüssel, der sogenannte öffentliche PublicKey(Trans);

v. ein dritter Schlüssel des Kundengerätes Sc, der sogenannte geheime PrivateKey(Cust) des Kunden, auch Verschlüsselungsschlüssel genannt;

vi. ein vierter Schlüssel des Kundengerätes Pc, der sogenannte öffentliche PublicKey(Cust) des Kunden, auch Entschlüsselungsschlüssel genannt;

vii. und die Datenelemente, welche das Kundengerät kennzeichnen:

a. eigene Telefonnummer (Phone#) und
b. IMEI (Hardwareidentifikationsnummer) und/oder die Kundennummer.

Das Verfahren läuft wie folgt ab:

i. In der Zentrale (oder auch Datenverarbeitungszentrale) wird genau ein RSA-Schlüsselpaar - Sa und Pa - erzeugt und gespeichert.

Jedoch werden für jedes Kundengerät zwei RSA-Schlüsselpaare neu generiert und gespeichert: Sc und Pc sowie St und Pt. Das Transportschlüsselpaar St-Pt wird zum gesicherten Transport des geheimen Kundenschlüssel Sc zum Kundengerät benötigt. Die Zentrale generiert auch für jeden Kunden das sogenannte Kundenzertifikat oder kurz Zertifikat. Die dafür notwendige Berechnungsvorschrift lautet: (1) verschlüssle eigene Phone#, IMEI (Hardwareidentifikationsnummer) und/oder die Kundennummer mit dem öffentlichen Kundenschlüssel Pc: ENC(Pc)(Phone#, IMEI, KuNu), (2) verschlüssle das Ergebnis aus (1) mit dem geheimen Schlüssel von Finalogic Sa: ENC(Sa)(ENC(Pc)(Phone#, IMEI (Hardwareidentifikationsnummer), KuNu)). Ein RSA-Schlüsselpaar

ist ein Schlüsselpaar, das aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft, besteht. Der private Schlüssel wird geheimgehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden. Ergebnis ist das Zertifikat „CustPK Certificate" für diesen Kunden. Im allgemeinen ist ein Zertifikat ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt sowie dessen Authentizität und Integrität durch kryptographische Verfahren geprüft werden können. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Fig. 1 zeigt diese Schritte und die Übermittlung an das Kundengerät, das als Mobiltelefon dargestellt ist. Gemeinsam mit einem für die Telefon- bzw. Kommunikationsgerätetype des Kunden geeigneten Programm (Application, kurz APP, oder auch telefonanbieterunabhängige Programm-Applikation auf Mobiltelefon oder Kommunikationsgerät) oder eines gleichwertigen Programmes, welches unter dem Gerätebetriebssystem laufen kann, werden die kryptographischen Elemente

- verschlüsselter geheimer Kundenschlüssel ENC(Pt)[Private Key(Cust) Sc] und
- Kundenzertifikat CustPK Certificate

zum Kundengerät funk- oder leitungstechnisch übermittelt.

Die Entgegennahme und Speicherung obiger Programme und Dateien auf der Festplatte des Kundengeräts bedarf der Zustimmung des Kunden.

Mit diesem Programm und diesen Informationen sind nun folgende Operationen durch den Kunden möglich:

Personalisierung:

Dieses Verfahren zur Authentifizierung ist nicht nur in der Lage, den zweifelsfreien Beweis zu liefern, daß zum Beispiel eine bestimmte Kauforder vom Kundengerät mit der einzigartigen Kundennummer oder der IMEI (Hardwareidentifikationsnummer) abgegeben wurden, sondern kann auch den Inhaber eineindeutig identifizieren.

Dazu wählt sich der Kunde seine persönliche PIN (Persönliche Identifikationsnummer) numerisch/alphanumerisch, wie international üblich zwischen 4 bis 12 Ziffern lang, für welche der Kunde selbst verantwortlich ist. Nur mit dieser PIN kann der Kunde alle Funktionen seiner APP nutzen.

Jedoch ist der Kunde bei der PIN-Eingabe auf mobilen Telefon- und Kommunikationsgeräten den betrügerischen Versuchen unlauterer Dritter zur Aufdeckung seiner PIN gefährdet. Hier besteht natürlich kein Unterschied zu anderen Systemen, die mit ähnlichen Schutzmechanismen zum Schutz der persönlichen Befugnisse ausgestattet sind. Daher gelten hierbei auch die gleichen Aufbewahrungsregeln von Paßwörtern.

Aus diesem Grund erfolgt die PIN- oder andere Zahleneingaben in dem erfindungsgemäßen Verfahren unter Verwendung der sogenannten verreihten PIN, wie in Fig. 2 dargestellt.

Auf der Bildschirmanzeige A des Kundengeräts wird dem Kunden - anstatt der üblichen Reichenfolge bzw. Anordnung der Ziffern 1 bis 9 und 0 - eine zufällige Anordnung dieser Ziffern gezeigt, gemäß dieser der Kunde auf der Gerätetastatur N seine PIN eingeben muß.

Beispiel 1 für numerische Tastaturen:
Die übliche Ziffernreihung lauten: 1234567890. Deren Anordnung sieht so aus wie in Fig. 3a dargestellt. Die verreihte Zif-

fernanordnung für diese PIN-Eingabe lautet gemäß Fig. 3b 6278015943. Für die verreihte Eingabe der PIN '7510' drückt der Kunde nun die Tastenfolge '3765'.

Beispiel 2 für numerische Tastaturen:
Hier ist noch ein Beispiel, um die Arbeitsweise der Methode der verreihten PIN zu demonstrieren. Die verreihte Ziffernanordnung für diese PIN-Eingabe lautet: 0768352419, wie in Fig. 3c gezeigt. Für die verreihte Eingabe der PIN '415597' drückt der Kunde nun '896602'.

Die zufällige Ziffernanforderungsvorschrift wechselt mit jeder PIN- oder anderen numerischen Dateneingabe (beispielsweise der Kreditkartennummer), nicht schon nach jeder Ziffer.

Das Verfahren der Personalisierung zur Sicherstellung der Echtheit der Identität des Absenders und Nutzers des Systems läuft wie folgt ab:

i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselentschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

ii. Anschließend generiert das Datenverarbeitungszentrum eine neue, beliebige Ziffernanordnung, beispielsweise '9243605718', wie in Fig. 3d dargestellt, und verschlüsselt sie mit dem öffentlichen Kundenschlüssel Pc gemäß ENC(Pc)(CustData,'9243605718'), und wird nun zum Kunden gesandt.

iii. Die APP entschlüsselt das erhaltene Chiffrat mit dem geheimen Kundenschlüssel Sc DEC(Sc)(ENC(Pc)(CustData, '9243605718')).

Am Bildschirm erscheint die neue Anordnungsvorschrift gemäß (ii) für die numerischen Tastaturbelegung, wie sie in Fig. 3d zu sehen ist.

iv. Der Kunde führt seine PIN-Eingabe gemäß der angezeigten Anordnungsvorschrift durch, das Ergebnis wird mit dem Verschlüsselungsschlüssel des Kunden Sc verschlüsselt. Auch das Zertifikat wird verschlüsselt: ENC(Sc)(CustPK Certificate,'397718'). Dies wird zur Zentrale gesendet.

v. In der Zentrale wird das Chiffrat geeignet entschlüsselt, und die PIN '415597' wird in den Stammdaten des Kunden gespeichert, sofern auch die Verifikation des Kundenzertifikats CustPK Certifiate erfolgreich war. Die Verifikation des Kundenzertifikats garantiert die Authentizität der übermittelten Daten und die Identität des Ursprungs.

Die PIN-Änderungsfunktion läuft wie folgt ab, denn ab nun kann der Kunde jederzeit auch die 'PIN-Änderungsfunktion' anwählen:

i. Eingabe der alten PIN
ii. Eingabe der neuen PIN
iii. Wiederholung der neuen PIN

Wesentlicher Vorteil dieser Methode ist, daß, weil Finalogic-System die Ziffernanordnungsvorschrift bei jeder Eingabe ändert, sich die Chiffrate der Schritte ii) und iii) wertemäßig unterscheiden - obwohl die Originalwerte ident sind.

Deswegen ist diese PIN-Änderungsfunktion sicherheitstechnisch den herkömmlichen Passwort-Änderungsfunktionen überlegen, da bei Finalogic-System eine sogenannte Datenwiedereinspielungsattacke erfolgreich erkannt und abgewehrt wird.

In der Praxis hat sich herausgestellt, daß sich Kunden die PIN nicht als Zahlenfolge merken, sondern als graphische Figur,

die der tippende Finger auf dem Ziffernblock ausführt. Daher kann eine ständig wechselnde Verreihung der Ziffern als unbequem empfunden werden und zu Eingabefehlern führen. Um dies zu vermeiden, kann der Kunde alternativ eine konkrete Verreihung der Ziffern wählen, die seinem Gerät vom Trust Server nutzerspezifisch zugewiesen und übermittelt wird. Die Verreihung der Ziffern wechselt also nicht nach jeder einzelnen Anwendung, sondern bleibt für den individuellen Kunden gleich. Dabei tritt der überraschende Effekt ein, daß die PIN-Eingabe weiterhin vor der Ausspähung Dritter weitgehend gesichert ist, aber gleichzeitig sich der Kunde eine graphische Figur, die sein tippender Finger beim Eingeben ausführt, merken kann und darf. Selbstverständlich kann der Nutzer jederzeit im Web-Registrierungsprozeß eine neue Verreihung vom Trust Server erstellen lassen oder zum System mit ständig wechselnder Verreihung der Ziffern wechseln, wenn ihm das aus Sicherheitsgründen geboten erscheint.

Die Transaktion für Rechtsgeschäfte läuft folgendermaßen ab:

1. Ablauf einer Einkaufstransaktion (Beispiel):

   i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselentschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

   ii. In der Datenverarbeitungszentrale wird ein Zeitstempel genommen, dieser wir mit dem öffentlichen Kundenschlüssel Pc verschlüsselt und zum Kunden gesandt, ENC(Pc)(CustData,'2010-07-01/10:09:11,571').

   iii. Die APP entschlüsselt das erhaltene Chiffrat mit dem geheimen Kundenschlüssel Sc DEC(Sc)(ENC(Pc)(CustData, '2010-07-01/10:09:11,571')).

Wird beispielsweise das Buch "Die Sieben Weltwunder" vom Kunden gewünscht, wird dessen ISBN Code zusammen mit dem Kundenzertifikat und dem Zeitstempel mit dem geheimen Kundenschlüssel Sc verschlüsselt, ENC(Sc)(CustPK Certificate,'2010-07-01/10:09:11,571','ISBN 3-8094-1694-0'), und zur Datenverarbeitungszentrale gesandt.

In der Datenverarbeitungszentrale wird das Chiffrat geeignet entschlüsselt, das Kundenzertifikat geprüft und, falls auch der Zeitstempel noch nicht zulange verstrichen ist, der Kaufauftrag des Kunden zum entsprechenden Händler weitergeleitet.

2. Ablauf einer Kreditkartenzahlung (Beispiel):

Wählt der Kunde als Option die Bezahlweise mittels Kreditkarten, kommt wieder unser gesichertes Verfahren mittels verreihter Ziffernanforderung zur Anwendung.

Die einzelnen Transaktionsschritte im Detail sind:

i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselverschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

ii. Die Zentrale generiert eine neue Ziffernanordnung, beispielsweise '9243605718', und verschlüsselt sie mit dem öffentlichen Kundenschlüssel Pc ENC(Pc)(CustData, '9243605718'), und wird zum Kunden gesandt.

iii. Die APP entschlüsselt das erhaltene Chiffrat mit dem geheimen Kundenschlüssel Sc gemäß DEC(Sc)(ENC(Pc)(CustData, '9243605718')).

Am Bildschirm erscheint die Anordnungsvorschrift, wie in Fig. 3d angegeben.

iv. Eingabe der Kartennummer, des Ablaufdatums und gegebenenfalls eines Prüfwertes gemäß der angezeigten Verreihungsvorschrift, das Ergebnis wird mit dem Verschlüsselungsschlüssel des Kunden Sc verschlüsselt, ENC(Sc)(CustPK Certificate, '7255236666666669', '92/94', '999'), und zur Zentrale gesandt.

v. In der Zentrale wird das Chiffrat geeignet entschlüsselt und das Kundenzertifikat geprüft und, falls positiv, wird eine entsprechende Kreditkartenzahlung initiiert.

Der Datenschutz ist ebenso gesichert, denn im System, das das erfindungsgemäße Verfahren verwendet, kommen sogenannte HSMs (Host Security Modules) zur Datenver- und Datenentschlüsselung und für die Schlüsselverwaltungsoperationen zum Einsatz.

Solche Geräte beinhalten für kryptographische Zwecke optimierte und vor jedem Angriff oder Zugriff von außen geschützte Rechen- und Speicherwerke. Ihr Schutzsystem geht soweit, daß sie keinesfalls Werte oder Instruktionen in unverschlüsselter Form nach außen lassen und alle Schlüsselwerte löschen, sobald jedweder Auslese- oder Datenabtastungsversuch erkannt wird. Auch die versuchte Entfernung einzelner Teile, ja sogar die unauthorisierte Öffnung des Gehäuses führt zum gesamten Speicherverlust - konkret wird dabei jedes Bit des Schlüsselspeichers mit '0' überschrieben.

Zum Schutz der persönlichen Daten unserer Kunden benutzt Finalogic im Datenverkehr mit den Händlern entweder

- eigene Leitungsverschlüsselungsschlüssel, falls die Gegenseite auch HSM-Module unterhält, oder

- zumindest SSL-Verschlüsselung zu den Datenempfangsgeräten der Händler, welche SSL verstehen müssen.

Die SSL-Verschlüsselung (Secure Socket Layer) wurde von den Firmen Netscape und RSA Data Security entwickelt. Das SSL-Protokoll soll gewährleisten, daß sensible Daten beim Surfen im Internet, beispielsweise Kreditkarten-Informationen beim Online Shopping, verschlüsselt übertragen werden. Somit soll verhindert werden, daß Dritt-Nutzer die Daten bei der Übertragung nicht auslesen oder manipulieren können. Zudem stellt dieses Verschlüsselungsverfahren die Identität einer Website sicher.

In den angesprochen Verschlüsselungsgeräten, etwa von Finalogic, findet eine Umschlüsselungsoperation unter Benutzung des Entschlüsselungsschlüssels des Kunden Pc und des Verschlüsselungsschlüssel des Händlers statt.

Sicherheitsanforderungskonforme HSMs müssen alle Sicherheitsanforderungen gemäß der internationalen Norm FIPS 140-2 Level 4 erfüllen. FIPS heißt Federal Information Processing Standard und ist die Bezeichnung für öffentlich bekanntgegebende Standars der Vereinigten Staaten. FIPS 140 impliziert, daß Datenmaterial im Klartext unter keinen Umständen ausgelesen oder sonst wie exportiert werden können.

Diese Vorgehensweise garantiert unseren Kunden vollkommenen Schutz ihrer persönlichen Daten während der Datenverarbeitung durch Finalogic.

Patentansprüche:

1. Verfahren zur Sicherung von Daten und Sicherstellung ihres Ursprungs, wobei die Daten von einem Kundengerät an eine Zentrale elektronisch verschlüsselt übermittelt werden, und wobei das Verfahren die folgenden Schritte umfaßt:

i) Erzeugen und Speichern eines RSA-Schlüsselpaares bestehend aus einem ersten Schlüssel (Sa) und einem zweiten Schlüssel (Pa) für das Signieren von Kundenzertifikaten in der Zentrale,

ii) Generieren und Speichern zweier RSA-Schlüsselpaare für das Kundengerät bestehend aus einem dritten Schlüssel des Kundengerätes (Sc) und einem vierten Schlüssel des Kundengerätes (Pc) sowie einem ersten Schlüsselverschlüsselungsschlüssel (St) und einem zweiten Schlüsselverschlüsselungsschlüssel (Pt), wobei der erste Schlüsselverschlüsselungsschlüssel (St) und der zweite Schlüsselverschlüsselungsschlüssel (Pt) zum gesicherten Transport des dritten Schlüssels des Kundengerätes (Sc) geeignet sind,

iii) Erzeugen eines verschlüsselten Schlüssels durch Verschlüsseln des dritten Schlüssels des Kundengerätes (Sc) mit dem zweiten Schlüsselverschlüsselungsschlüssel (Pt) sowie Generieren eines Kundenzertifikats in der Zentrale durch Verschlüsseln der kundenspezifischen Telefonnummer sowie der IMEI des Kundengerätes und/oder einer Kundennummer mit dem vierten Schlüssel des Kundengerätes (Pc) und anschließendem Verschlüsseln mit dem ersten Schlüssel (Sa) für das Signieren von Kundenzertifikaten,

iv) Übermitteln des verschlüsselten Schlüssels und des Kundenzertifikats an das Kundengerät,

v) Senden des ersten Schlüsselverschlüsselungsschlüssels (St) an das Kundengerät nach einer Anforderung durch das Kundengerät,

vi) Entschlüsseln des verschlüsselten Schlüssels mit dem ersten Schlüsselverschlüsselungsschlüssel (St) in dem Kundengerät, wobei der dritte Schlüssel des Kundengerätes (Sc) erhalten wird,

vii) Verschlüsseln einer verreihten Ziffernanordnung in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc),

viii) Senden der verschlüsselten verreihten Ziffernanordnung an das Kundengerät,

ix) Entschlüsseln der verschlüsselten verreihten Ziffernanordnung im Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc),

x) Verschlüsseln einer ersten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat,

xi) Senden des Chiffrats und des Kundenzertifikats an die Zentrale,

xii) Entschlüsseln des Chiffrats in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc), Entschlüsseln der ersten PIN-Eingabe und Überprüfen des zugesendeten Kundenzertifikats mit dem in der Zentrale gespeicherten Kundenzertifikat.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Chiffrat in der Zentrale entschlüsselt und daß das vom Kundengerät übermittelte Zertifikat mit dem in der Zentrale gespeicherten Zertifikat verglichen wird, um die Authentizität der Daten zu verifizieren.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Übermittlung der Daten von der Zentrale an das Kundengerät und vom Kundengerät an die Zentral per Funk- und/oder per Leitungsverbindung erfolgt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Verreihung der verreihten Ziffernanordnung bei der Initialisierung des Verfahrens einmalig vom Kunden gewählt und an die Zentrale übermittelt wird.

5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Verreihung der verreihten Ziffernanordnung in der Zentrale für jede Übermittlung an das Kundengerät neu generiert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, gekennzeichnet durch die weiteren Schritte

iii.a) Generieren eines Zeitstempels in der Zentrale,
iv.a) Übermitteln des verschlüsselten Schlüssels zusammen mit dem Zeitstempel an das Kundengerät,
x.a) Verschlüsseln der ersten PIN-Eingabe am Kundengerät zusammen mit dem Zeitschlüssel zu einem Chiffrat.

7. Verfahren nach einem der Ansprüche 1 bis 6, gekennzeichnet durch die weiteren Schritte:

x.b) Verschlüsseln einer zweiten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes

(Sc) zu einem Chiffrat, um eine neue PIN zur Zentrale zu schicken, und

x.c) Verschlüsseln einer dritten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat, um die neue PIN zu bestätigen.

8. Verfahren nach einem der Ansprüche 1 bis 6, gekennzeichnet dadurch, daß zusätzlich zur ersten PIN-Eingabe die Nummerneingabe einer Kreditkartennummer und/oder ein Ablaufdatum einer Kreditkarte und/oder eine Prüfziffer einer Kreditkarte erfolgt und zusammen mit der ersten PIN-Eingabe verschlüsselt an die Zentrale übermittelt wird.

9. Verfahren nach einem der Ansprüche 1 bis 6, gekennzeichnet dadurch, daß zusätzlich zur ersten PIN-Eingabe die Nummerneingabe einer warenspezifischen Zahl, wie z.B. die ISBN eines Buchtitels, erfolgt und zusammen mit der ersten PIN-Eingabe verschlüsselt an die Zentrale übermittelt wird.

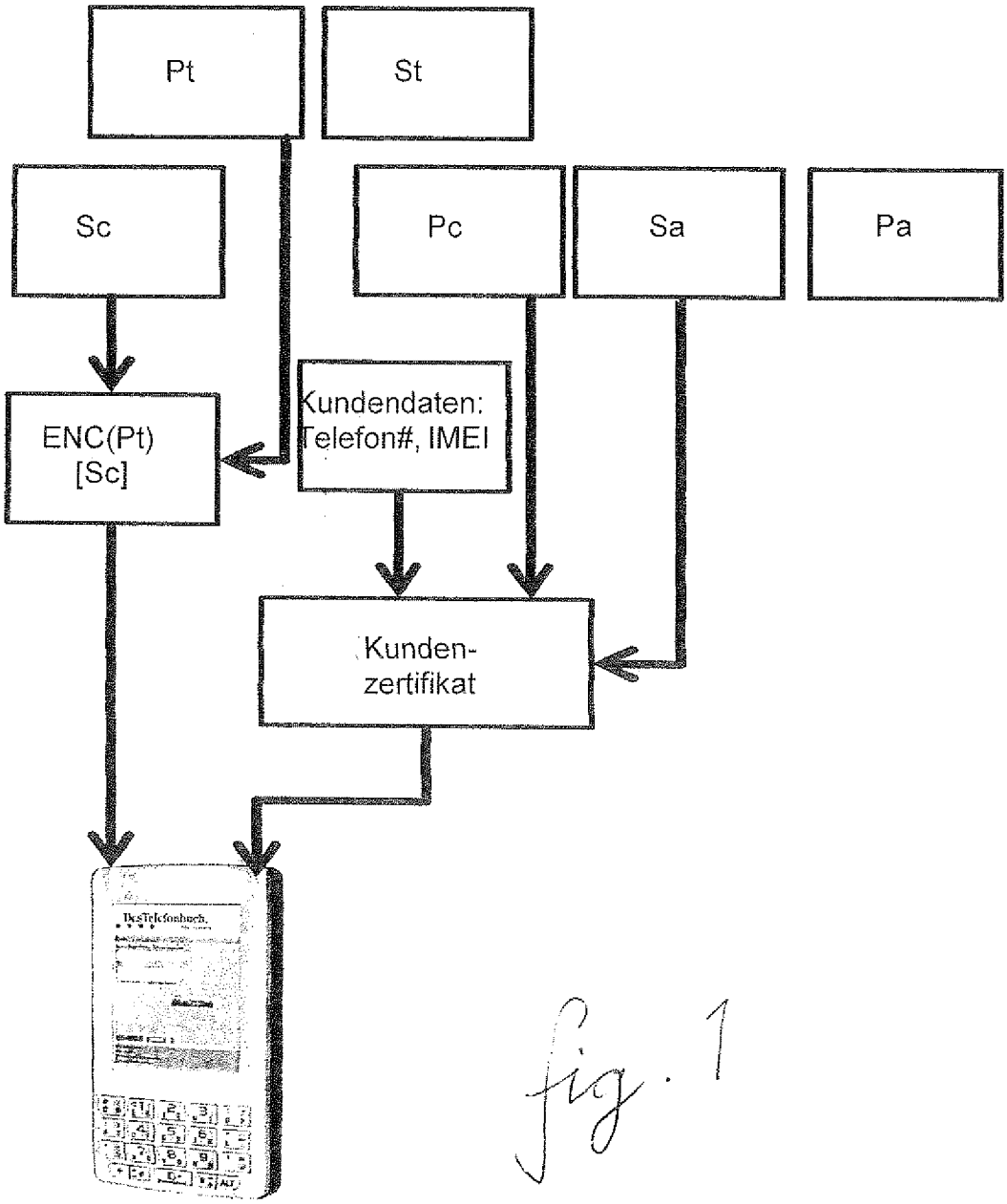

Pt
St
Sc
Pc
Sa
Pa
ENC(Pt)
[Sc]
Kundendaten:
Telefon#, IMEI
Kunden-
zertifikat

fig. 1

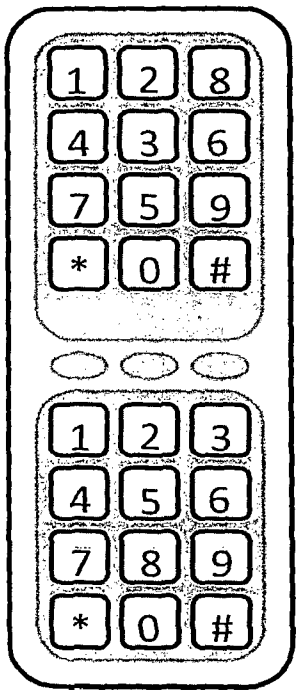


fig. 2

1 2 3	6 2 7	0 7 6	9 2 4
4 5 6	8 0 1	8 3 5	3 6 0
7 8 9	5 9 4	2 4 1	5 7 1
* 0 #	* 3 #	* 9 #	* 8 #

fig. 3a 3b 3c 3d

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2013/000013

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06
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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/168055 A1 (LORD ROBERT B [US] ET AL) 26 August 2004 (2004-08-26) paragraph [0120] - paragraph [0124] paragraph [0139] - paragraph [0162] paragraph [0178] - paragraph [0194] paragraph [0340] - paragraph [0346]; claims 1-4,25-28; figures 3-6	1-9

-/--

[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
28 March 2013	09/04/2013

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	Schwibinger, Hans

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2013/000013

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DI NATALE G ET AL: "A Reliable Architecture for the Advanced Encryption Standard", PROCEEDINGS 13TH IEEE EUROPEAN TEST SYMPOSIUM - ETS 2008 - 25-29 MAY 2008, VERBANIA, ITALY, IEEE, NEW YORK, NY, US, 25 May 2008 (2008-05-25), pages 13-18, XP031281076, ISBN: 978-0-7695-3150-2 page 14, left-hand column, line 8 - page 15, left-hand column, line 8; figure 1	1-9
A	WO 02/47356 A2 (THOMSON LICENSING SA [FR]; ANDREAUX JEAN PIERRE [FR]; CHEVREAU SYLVAIN) 13 June 2002 (2002-06-13) page 2, line 11 - line 25 page 3, line 1 - line 20 page 5, line 33 - page 6, line 29 page 10, line 36 - page 11, line 8; claims 1,5-7,10,11; figures 2-4	1-9
A	GB 2 457 367 A (CONNOTECH EXPERTS CONSEILS INC [CA]) 19 August 2009 (2009-08-19) paragraph [0019] - paragraph [0026] paragraph [0049] - paragraph [0063]; figures 2-41-3,10-19	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/AT2013/000013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004168055 A1	26-08-2004	US 2004168055 A1	26-08-2004
		US 2007050624 A1	01-03-2007
		US 2010223470 A1	02-09-2010
		US 2013036302 A1	07-02-2013
		WO 2004075031 A2	02-09-2004
WO 0247356 A2	13-06-2002	AU 2960102 A	18-06-2002
		BR 0115979 A	06-01-2004
		CN 1478350 A	25-02-2004
		EP 1348291 A2	01-10-2003
		FR 2818062 A1	14-06-2002
		HU 0303569 A2	28-01-2004
		JP 4714402 B2	29-06-2011
		JP 2004515972 A	27-05-2004
		MX PA03004804 A	10-09-2003
		PL 362175 A1	18-10-2004
		US 2004083364 A1	29-04-2004
		WO 0247356 A2	13-06-2002
		ZA 200304024 A	24-06-2003
GB 2457367 A	19-08-2009	CA 2621147 A1	15-08-2009
		GB 2457367 A	19-08-2009
		US 2009210696 A1	20-08-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2013/000013

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/06
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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2004/168055 A1 (LORD ROBERT B [US] ET AL) 26. August 2004 (2004-08-26) Absatz [0120] - Absatz [0124] Absatz [0139] - Absatz [0162] Absatz [0178] - Absatz [0194] Absatz [0340] - Absatz [0346]; Ansprüche 1-4,25-28; Abbildungen 3-6	1-9

-/--

[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
28. März 2013	09/04/2013

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	Schwibinger, Hans

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DI NATALE G ET AL: "A Reliable Architecture for the Advanced Encryption Standard", PROCEEDINGS 13TH IEEE EUROPEAN TEST SYMPOSIUM - ETS 2008 - 25-29 MAY 2008, VERBANIA, ITALY, IEEE, NEW YORK, NY, US, 25. Mai 2008 (2008-05-25), Seiten 13-18, XP031281076, ISBN: 978-0-7695-3150-2 Seite 14, linke Spalte, Zeile 8 - Seite 15, linke Spalte, Zeile 8; Abbildung 1	1-9
A	WO 02/47356 A2 (THOMSON LICENSING SA [FR]; ANDREAUX JEAN PIERRE [FR]; CHEVREAU SYLVAIN) 13. Juni 2002 (2002-06-13) Seite 2, Zeile 11 - Zeile 25 Seite 3, Zeile 1 - Zeile 20 Seite 5, Zeile 33 - Seite 6, Zeile 29 Seite 10, Zeile 36 - Seite 11, Zeile 8; Ansprüche 1,5-7,10,11; Abbildungen 2-4	1-9
A	GB 2 457 367 A (CONNOTECH EXPERTS CONSEILS INC [CA]) 19. August 2009 (2009-08-19) Absatz [0019] - Absatz [0026] Absatz [0049] - Absatz [0063]; Abbildungen 2-41-3,10-19	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/AT2013/000013

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2004168055 A1	26-08-2004	US 2004168055 A1	26-08-2004
		US 2007050624 A1	01-03-2007
		US 2010223470 A1	02-09-2010
		US 2013036302 A1	07-02-2013
		WO 2004075031 A2	02-09-2004
WO 0247356 A2	13-06-2002	AU 2960102 A	18-06-2002
		BR 0115979 A	06-01-2004
		CN 1478350 A	25-02-2004
		EP 1348291 A2	01-10-2003
		FR 2818062 A1	14-06-2002
		HU 0303569 A2	28-01-2004
		JP 4714402 B2	29-06-2011
		JP 2004515972 A	27-05-2004
		MX PA03004804 A	10-09-2003
		PL 362175 A1	18-10-2004
		US 2004083364 A1	29-04-2004
		WO 0247356 A2	13-06-2002
		ZA 200304024 A	24-06-2003
GB 2457367 A	19-08-2009	CA 2621147 A1	15-08-2009
		GB 2457367 A	19-08-2009
		US 2009210696 A1	20-08-2009