(19) österreichisches patentamt

(10) **AT 512 289 B1 2013-07-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 131/2012
(22) Anmeldetag: 31.01.2012
(45) Veröffentlicht am: 15.07.2013

(51) Int. Cl. : ***H04L 9/32*** (2006.01)
G06F 21/33 (2013.01)
G07F 7/10 (2006.01)
H04L 12/28 (2006.01)

(56) Entgegenhaltungen:
US 2002029342 A1
US 2003182558 A1
WO 2003096165 A2
WO 2008067575 A1
US 2008148186 A1
US 2008298588 A1
EP 1615181 A1

(73) Patentinhaber:
FINALOGIC BUSINESS TECHNOLOGIES GMBH
1010 WIEN (AT)

(72) Erfinder:
BEIDL HEINRICH MAG.
WIEN (AT)
HRDY ERWIN
DEUTSCH WAGRAM (AT)
SCHAUERHUBER JULIUS ING.
ABSDORF (AT)

(54) **KRYPTOGRAPHISCHES AUTHENTIFIZIERUNGS- UND IDENTIFIKATIONSVERFAHREN FÜR MOBILE TELEFON- UND KOMMUNIKATIONSGERÄTE MIT REALZEITVERSCHLÜSSELUNG WÄHREND DER AKTIONSPERIODE**

(57) Verfahren zur Sicherung von Daten und Sicherstellung ihres Ursprungs , wobei die Daten von einem Kundengerät an eine Zentrale elektronisch verschlüsselt übermittelt werden.

.

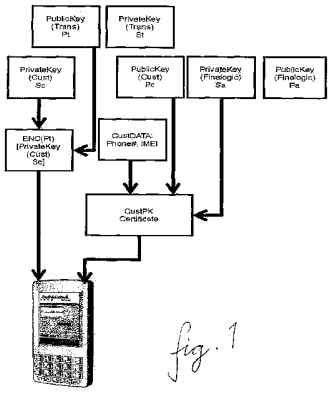

fig. 1

AT 512 289 B1 2013-07-15

Beschreibung

[0001] 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.

[0002] Im Stand der Technik sind Verfahren zur sicheren Übermittlung elektronischer Daten mit Hilfe von digitalen Verschlüsselungstechniken bekannt.

[0003] 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.

[0004] Die AT 504 634 B1 sowie die WO 2008 151 209 A1, auch veröffentlicht als US 2 008 2 98 58 8 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.

[0005] 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.

[0006] 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.

[0007] 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.

[0008] 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).

[0009] Die Aufgaben werden erfindungsgemäß dadurch erreicht, dass das Verfahren die folgenden Schritte umfasst:

[0010] 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,

[0011] 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,

[0012] 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,

[0013] iv) Übermitteln des verschlüsselten Schlüssels und des Kundenzertifikats an das Kundengerät,

[0014] v) Senden des ersten Schlüsselverschlüsselungsschlüssels (St) an das Kundengerät nach einer Anforderung durch das Kundengerät,

[0015] vi) Entschlüsseln des verschlüsselten Schlüssels mit dem ersten Schlüsselverschlüsselungsschlüssel (St) in dem Kundengerät, wobei der dritte Schlüssel des Kundengerätes (Sc) erhalten wird,

[0016] vii) Verschlüsseln einer verreihten Ziffernanordnung in der Zentrale mit dem vierten Schlüssel des Kundengerätes (Pc),

[0017] viii) Senden der verschlüsselten verreihten Ziffernanordnung an das Kundengerät,

[0018] ix) Entschlüsseln der verschlüsselten verreihten Ziffernanordnung im Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc),

[0019] x) Verschlüsseln einer ersten PIN-Eingabe am Kundengerät mit dem dritten Schlüssel des Kundengerätes (Sc) zu einem Chiffrat,

[0020] xi) Senden des Chiffrats und des Kundenzertifikats an die Zentrale,

[0021] 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.

[0022] 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.

[0023] 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.

[0024] 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.

[0025] Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens, dass das Verfahren die weiteren Schritte umfasst:

[0026] iii.a) Generieren eines Zeitstempels in der Zentrale,

[0027] iv.a) Übermitteln des verschlüsselten Schlüssels zusammen mit dem Zeitstempel an das Kundengerät,

[0028] x.a) Verschlüsseln der ersten PIN-Eingabe am Kundengerät zusammen mit dem Zeitschlüssel zu einem Chiffrat.

[0029] Eine bevorzugte Ausführungsform des Verfahrens zeichnet sich durch die weiteren Schritte aus:

[0030] 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

[0031] 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.

[0032] 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.

[0033] 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.

[0034] Die Erfindung wird nachstehend anhand eines in den Zeichnungen dargestellten Ausführungsbeispiels näher erläutert. Es zeigen:

[0035] Fig. 1 eine schematische Darstellung der Übermittlung vorbereitender Daten an ein Kundengerät,

[0036] Fig. 2 ein schematisches Kundengerät, und die

[0037] Fig. 3a bis 3d verschieden verreihte Ziffernanordnungen auf einem Nummernfeld.

[0038] 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.

[0039] Dies betrifft folglich den Schutz von numerischen und/oder auch alphanumerischen Dateneingaben an mobilen Telefon- und Kommunikationsgeräte vor Kenntnisnahme unberechtigter Dritter.

[0040] Solche Dateneingaben können sein und werden in dem Verfahren angewendet bei der

[0041] • Festlegung, Eingabe und Änderung der PIN des Mobiltelefonhalters und der

[0042] • Eingabe von Kreditkartendaten des Mobiltelefon- bzw. Kommunikationsgerätehalters.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] Abschließend wird der Kunde noch um zwei Datenelemente seines Geräts gefragt:

[0047] i. die eigene Telefonnummer (Phone#) und

[0048] 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.

[0049] 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.

[0050] Nach Eingabe dieser Informationen in das Finalogic-System ist der Registrierungsprozess beendet.

[0051] 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.

[0052] 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.

[0053] Folgende asymmetrische Schlüsselpaare finden Verwendung:

[0054] i. ein erster Schlüssel für das Signieren von Kundenzertifikaten Sa, der sogenannte geheime PrivateKey(Finalogic);

[0055] ii. ein zweiter Schlüssel Pa für das Signieren von Kundenzertifikaten, der sogenannte öffentliche PublicKey(Finalogic);

[0056] iii. ein erster Schlüsselverschlüsselungsschlüssel St, der sogenannte geheime PrivateKey(Trans);

[0057] iv. ein zweiter Schlüsselverschlüsselungsschlüssel, der sogenannte öffentliche PublicKey(Trans);

[0058] v. ein dritter Schlüssel des Kundengerätes Sc, der sogenannte geheime PrivateKey(Cust) des Kunden, auch Verschlüsselungsschlüssel genannt;

[0059] vi. ein vierter Schlüssel des Kundengerätes Pc, der sogenannte öffentliche PublicKey(Cust) des Kunden, auch Entschlüsselungsschlüssel genannt;

[0060] vii. und die Datenelemente, welche das Kundengerät kennzeichnen:

a. eigene Telefonnummer (Phone#) und

b. IMEI (Hardwareidentifikationsnummer) und/oder die Kundennummer.

[0061] Das Verfahren läuft wie folgt ab:

[0062] i. In der Zentrale (oder auch Datenverarbeitungszentrale) wird genau ein RSA-Schlüsselpaar - Sa und Pa - erzeugt und gespeichert.

[0063] 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 gesicher-

ten 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

[0064] • verschlüsselter geheimer Kundenschlüssel ENC(Pt)[Private Key(Cust) Sc] und

[0065] • Kundenzertifikat CustPK Certificate

[0066] zum Kundengerät funk- oder leitungstechnisch übermittelt.

[0067] Die Entgegennahme und Speicherung obiger Programme und Dateien auf der Festplatte des Kundengeräts bedarf der Zustimmung des Kunden.

[0068] Mit diesem Programm und diesen Informationen sind nun folgende Operationen durch den Kunden möglich:

[0069] Personalisierung:

[0070] 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.

[0071] 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.

[0072] 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.

[0073] Aus diesem Grund erfolgt die PIN- oder andere Zahleneingaben in dem erfindungsgemäßen Verfahren unter Verwendung der sogenannten verreihten PIN, wie in Fig. 2 dargestellt.

[0074] 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.

[0075] Beispiel 1 für numerische Tastaturen:

[0076] Die übliche Ziffernreihung lauten: 1234567890. Deren Anordnung sieht so aus wie in Fig. 3a dargestellt. Die verreihte Ziffernanordnung für diese PIN-Eingabe lautet gemäß Fig. 3b

6278015943. Für die verreihte Eingabe der PIN '7510' drückt der Kunde nun die Tastenfolge '3765'.

[0077] Beispiel 2 für numerische Tastaturen:

[0078] 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'.

[0079] Die zufällige Ziffernanforderungsvorschrift wechselt mit jeder PIN- oder anderen numerischen Dateneingabe (beispielsweise der Kreditkartennummer), nicht schon nach jeder Ziffer.

[0080] Das Verfahren der Personalisierung zur Sicherstellung der Echtheit der Identität des Absenders und Nutzers des Systems läuft wie folgt ab:

[0081] i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselentschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] Die PIN-Änderungsfunktion läuft wie folgt ab, denn ab nun kann der Kunde jederzeit auch die 'PIN-Änderungsfunktion' anwählen:

[0087] i. Eingabe der alten PIN

[0088] ii. Eingabe der neuen PIN

[0089] iii. Wiederholung der neuen PIN

[0090] 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.

[0091] Deswegen ist diese PIN-Änderungsfunktion sicherheitstechnisch den herkömmlichen Passwort-Änderungsfunktionen überlegen, da bei Finalogic-System eine sogenannte Datenwiedereinspielungsattacke erfolgreich erkannt und abgewehrt wird.

[0092] 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 An-

wendung, 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.

[0093] Die Transaktion für Rechtsgeschäfte läuft folgendermaßen ab:

[0094] 1. Ablauf einer Einkaufstransaktion (Beispiel):

[0095] i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselentschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

[0096] 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').

[0097] iii. Die APP entschlüsselt das erhaltene Chiffrat mit dem geheimen Kundenschlüssel Sc DEC(Sc)(ENC(Pc)(CustData, '2010-07-01/10:09:11, 571')).

[0098] Wird beispielsweise das Buch "Die Sieben Weltwunder" vom Kunden gewünscht, wird dessen ISBN Code zusammen mit dem Kunden-Zertifikat 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.

[0099] In der Datenverarbeitungszentrale wird das Chiffrat geeignet entschlüsselt, das Kundenzertifikat geprüft und, falls auch der Zeitstempel noch nicht zulange verstrichen ist, der Kauf -auftrag des Kunden zum entsprechenden Händler weitergeleitet.

[00100] 2. Ablauf einer Kreditkartenzahlung (Beispiel):

[00101] Wählt der Kunde als Option die Bezahlweise mittels Kreditkarten, kommt wieder unser gesichertes Verfahren mittels verreihter Ziffernanforderung zur Anwendung.

[00102] Die einzelnen Transaktionsschritte im Detail sind:

[00103] i. Unmittelbar nach Öffnung der APP wird von der Zentrale der geheime Schlüsselverschlüsselungsschlüssel St angefordert, um den eigentlichen Verschlüsselungsschlüssel Sc des Kunden zu erhalten.

[00104] 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.

[00105] 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.

[00106] 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.

[00107] v. In der Zentrale wird das Chiffrat geeignet entschlüsselt und das Kundenzertifikat geprüft und, falls positiv, wird eine entsprechende Kreditkartenzahlung initiiert.

[00108] 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.

[00109] Solche Geräte beinhalten für kryptographische Zwecke optimierte und vor jedem An-

griff 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.

[00110] Zum Schutz der persönlichen Daten unserer Kunden benutzt Finalogic im Datenverkehr mit den Händlern entweder

[00111] • eigene Leitungsverschlüsselungsschlüssel, falls die Gegenseite auch HSM-Module unterhält, oder

[00112] • zumindest SSL-Verschlüsselung zu den Datenempfangsgeräten der Händler, welche SSL verstehen müssen.

[00113] 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.

[00114] In den angesprochen Verschlüsselungsgeräten, etwa von Finalogic, findet eine Umschlüsselungsoperation unter Benutzung des Entschlüsselungsschlüssels des Kunden Pc und des Verschlüsselungsschlüssel des Händlers statt.

[00115] 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.

[00116] 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 Kunden-Zertifikats 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.

Hierzu 3 Blatt Zeichnungen

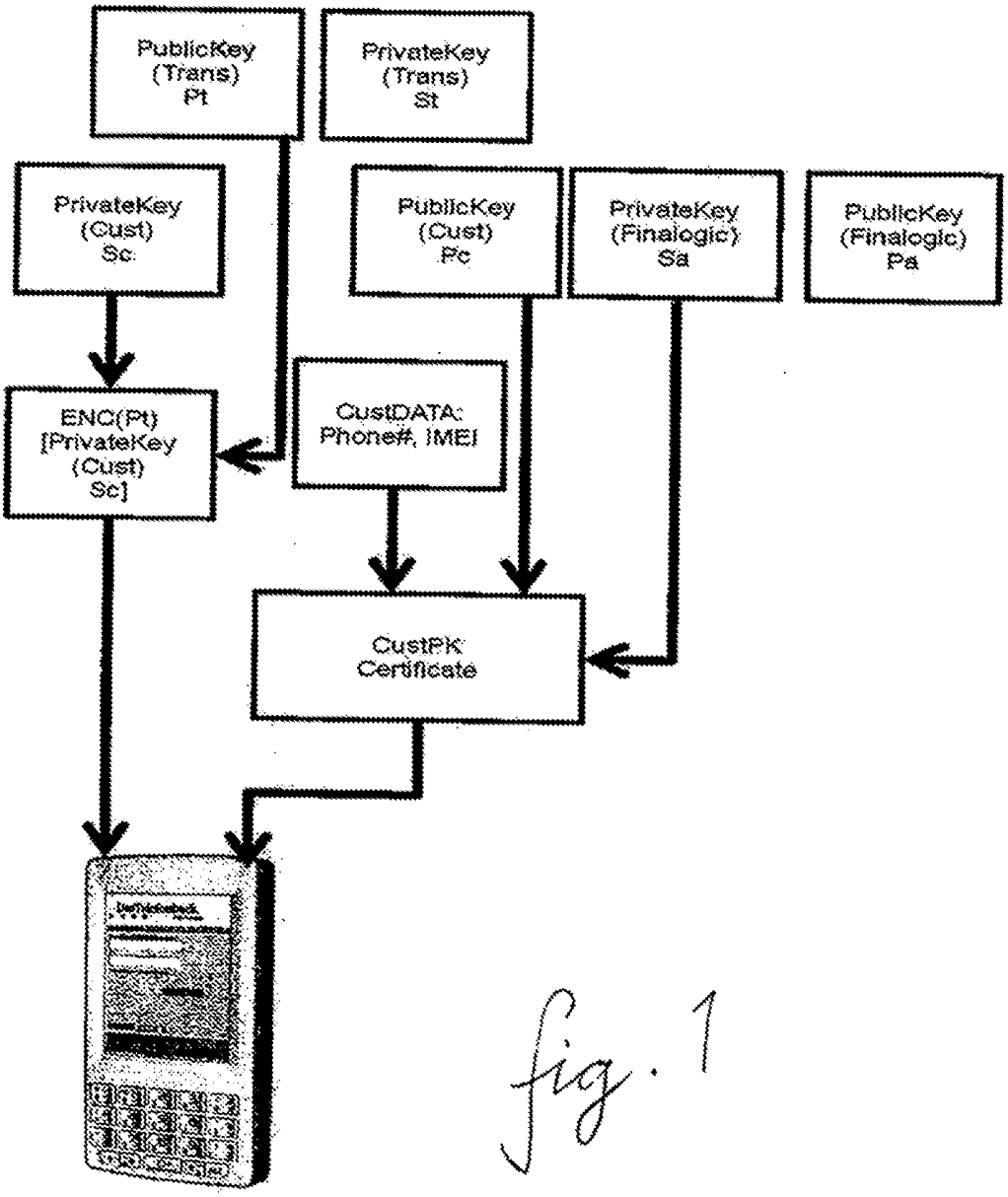
PublicKey (Trans) Pt
PrivateKey (Trans) St
PrivateKey (Cust) Sc
PublicKey (Cust) Pc
PrivateKey (Finalogic) Sa
PublicKey (Finalogic) Pa
ENC(Pt) [PrivateKey (Cust) Sc]
CustDATA: Phone#, IMEI
CustPK Certificate

fig. 1

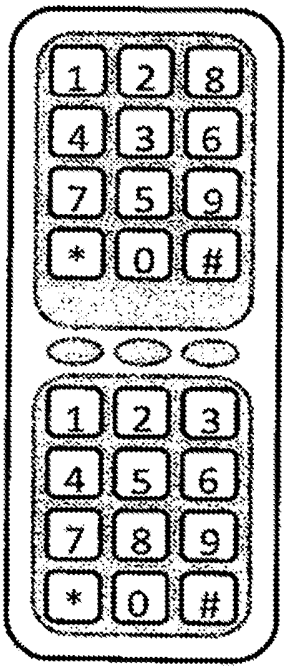

fig. 2

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