(19) österreichisches patentamt

(10) **AT 504 634 B1 2008-11-15**

(12) # Patentschrift

(21) Anmeldenummer: A 2004/2006

(22) Anmeldetag: 2006-12-04

(43) Veröffentlicht am: 2008-11-15

(51) Int. Cl.[8]: ***G07F 7/10*** (2006.01)
G06Q 20/00 (2006.01)
G06Q 30/00 (2006.01)
H04L 9/32 (2006.01)

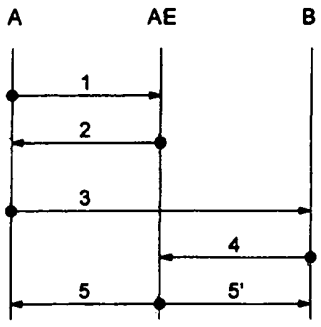
(56) Entgegenhaltungen:
US 5999625A WO 2001/001361A1
WO 2003/046685A2

(73) Patentanmelder:
HOFSTÄDTER GERNOT DR.
A-6020 INNSBRUCK (AT)

(54) **VERFAHREN ZUM TRANSFERIEREN VON VERSCHLÜSSELTEN NACHRICHTEN**

(57) Verfahren zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern (A, B), insbesondere kryptografisches Protokoll, wobei die Transaktion der Nachrichten unter Zwischenschaltung einer Authentifizierungseinrichtung erfolgt, welche die von den Anwendern (A, b) erhaltenen Nachrichten entschlüsselt und wiederum insbesondere verschlüsselte Nachrichten an die Anwender (A, B) sendet und folgende Schritte umfasst: Senden einer Nachricht (NA_1) durch einen ersten Anwender (A) an die Authentifizierungseinrichtung (AE), Erstellen eines Transaktionsidentifikationsdatensatzes (T_{ID}) durch die Authentifizierungseinrichtung (AE), Senden einer den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NAE_1) durch die Authentifizierungseinrichtung (AE) an den ersten Anwender (A), Erstellen einer mit einem Schlüssel (SA_2) verschlüsselten, den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NA_2) durch den ersten Anwender (A); Senden der Nachricht (NA_2) an einen zweiten Anwender (B), Erstellen einer die verschlüsselte Nachricht (NA_2) beinhaltenden, mit einem weiteren Schlüssel (SB) verschlüsselten Nachricht (NB_1) durch den zweiten Anwender (B), Senden der Nachricht (NB_1) an die Authentifizierungseinrichtung (AE), Entschlüsseln der Nachricht (NB_1), (NA_2) unter Verwendung der entsprechenden Schlüssel (SB_1), (SA_2) durch die Authentifizierungseinrichtung (AE), Erstellen einer Nachricht (NAE_2) durch die Authentifizierungseinrichtung (AE) unter Bezugnahme auf die in den entschlüsselten Nachrichten (NA_2), (NB_1) enthaltenen Klartexte (A_2), (B_1) und Senden der Nachricht (NAE_2) an den ersten Anwender (A) und/oder den zweiten Anwender (B).

Fig. 1a



AT 504 634 B1 2008-11-15

Die Erfindung betrifft ein Verfahren zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern, insbesondere kryptografisches Protokoll, wobei die Transaktion der Nachrichten unter Zwischenschaltung einer Authentifizierungseinrichtung erfolgt, welche die von den Anwendern erhaltenen Nachrichten entschlüsselt und wiederum insbesondere verschlüsselte Nachrichten an die Anwender sendet.

Verfahren zum Transferieren von verschlüsselten Nachrichten sind seit Langem bekannt, wobei die Sicherheit der so genannten kryptografischen Verfahren auf der Komplexität der eingesetzten Transformationen und der Geheimhaltung der Schlüssel basiert. Wesentliche Ziele der modernen Kryptografie sind zum Ersten, dass nur dazu berechtigte Personen in der Lage sein sollten, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen, zum Zweiten sollte der Urheber der Daten bzw. der Absender der Nachricht eindeutig identifizierbar sein und nicht in der Lage sein, seine Urheberschaft zu bestreiten, und zum Dritten sollte sichergestellt sein, dass die Daten nach ihrer Erzeugung nicht unberechtigterweise verändert wurden.

Die Gesamtheit der kryptografischen Verfahren, die einen sicheren Transport einer Nachricht vom Sender zum Empfänger mittels Verschlüsselung gewährleisten, bezeichnet man als Kryptosystem, das mathematisch gesehen aus einer Nachricht, einem Geheimtext, dem Schlüssel und Funktionen zur Chiffrierung und Dechiffrierung besteht. Dabei hängt die Sicherheit eines Kryptosystemes in der Regel von der Größe des Schlüsselraumes und von der Güte der Chiffrierfunktion ab.

Grundsätzlich lassen sich die zum Einsatz kommenden Kryptosysteme in symmetrische, asymmetrische und hybride Kryptosysteme einteilen. Symmetrische Kryptosysteme zeichnen sich dadurch aus, dass der Chiffrierschlüssel und der Dechiffrierschlüssel gleich oder zumindest leicht voneinander ableitbar sind, während bei asymmetrischen Kryptosystemen die verwendeten Algorithmen so gewählt sind, dass zwischen einem Chiffrierschlüssel und dem zugehörigen Dechiffrierschlüssel kein trivialer Zusammenhang besteht, sodass es nicht möglich ist, vom Chiffrierschlüssel direkt auf den Dechiffrierschlüssel zu schließen. Hybride Kryptosysteme versuchen, die Vorteile der symmetrischen und asymmetrischen Systeme zu verbinden, wobei in der Regel der Nachrichtenaustausch mittels eines schnellen symmetrischen Verfahrens stattfindet, während für den Austausch des Sitzungsschlüssel ein asymmetrisches Verfahren verwendet wird.

Symmetrischen Kryptosystemen haftet das Problem der Schlüsselverteilung an, das darin besteht, den Kommunikationspartnern einen gemeinsamen, geheimen Schlüssel zugänglich zu machen.

Das Schlüsselverteilungsproblem existiert bei asymmetrischen Verschlüsselungssystemen, die auf der so genannten Public-Key-Verschlüsselung beruhen, nicht. Das Prinzip der geheimen Schlüssel wird dabei völlig auf den Kopf gestellt, da jeder den öffentlichen Schlüssel kennt oder hat. Es kann aber nur einer die Nachricht mit dem dazugehörigen privaten Schlüssel lesen. Das heißt, der Sender verschlüsselt mit dem Public-Key des Empfängers, der jedermann bekannt sein kann. Der Empfänger entschlüsselt danach mit seinem geheimen Private-Key.

So sicher die Public-Key Verschlüsselung auch ist, gibt es dennoch Schwachstellen im vertraulichen Informationsaustausch. Da der Public-Key jedem bekannt ist, ist es möglich, verschlüsselte Nachrichten auch unter falschem Namen zuzusenden. Es fehlt also eine richtige Unterschrift, die den Schreiber identifiziert bzw. die Echtheit des Dokumentes bestätigt. Aus diesem Grund ist es bei asymmetrischen Kryptosystemen notwendig, dass der Absender mit seinem privaten Schlüssel eine Signatur erzeugt, die er dem Dokument beifügt. Diese Signatur kann vom Empfänger mit dem öffentlichen Schlüssel überprüft und so die Echtheit des Absenders verifiziert werden.

Der Ablauf des Datentransfers erfolgt in der Regel gemäß einem Protokoll, das eine eindeutige und zweifelsfreie Handlungsanweisung an die Beteiligten darstellt. Um sinnvoll eingesetzt werden zu können muss ein Protokoll durchführbar sein, d.h., wenn sich alle Beteiligten an die Spezifikation halten, muss das gewünschte Ergebnis erzielt werden. Weiters sollte das Protokoll die Korrektheit gewährleisten, d.h., wenn ein Teilnehmer versucht zu betrügen, muss dieser Versuch mit hoher Wahrscheinlichkeit zu erkennen sein.

Ein häufig verwendetes Protokoll aus dem Bereich der Kryptografie, bei dem zwei Kommunikationspartner einen geheimen Schlüssel, den nur diese beiden kennen, erzeugen, stellt der so genannte Diffie-Hellmann-Schlüsselaustausch dar. Der nach diesem Prinzip erzeugte Schlüssel wird üblicherweise verwendet, um verschlüsselte Nachrichten mittels eines symmetrischen Kryptosystemes zu übertragen. Der Diffie-Hellmann-Schlüsselaustausch basiert auf der Überlegung, dass etwas in der einen Richtung leicht zu tun, in der entgegengesetzten Richtung aber nur sehr schwer zu tun ist. Mathematisch ausgedrückt basiert der Diffie-Hellmann-Schlüsselaustausch also auf einer Einwegfunktion, wobei die Aufgabenstellung nur mit enormem Rechenaufwand zu lösen ist, wodurch ein Angreifer auch in Kenntnis der einzelnen unverschlüsselt übertragenen Nachrichten nicht in der Lage ist, den erzeugten Schlüssel zu berechnen. Allerdings ist der Diffie-Hellmann-Schlüsselaustausch dann nicht mehr sicher, wenn es einem Angreifer bei einem so genannten Man-In-The-Middle-Angriff gelingt, Datenpakete zu verändern.

Praktisch heißt das, dass der Angreifer die von A und B gesendeten Nachrichten abfängt und jeweils eigene Nachrichten weitersendet. Das heißt, im Prinzip wird zweimal ein Diffie-Hellmann-Schlüsselaustausch durchgeführt, und zwar einmal zwischen dem Anwender A und dem Angreifer, und einmal zwischen dem Angreifer und dem Anwender B. Da die Anwender A und B davon ausgehen, mit dem jeweils anderen Anwender zu kommunizieren, kann der Angreifer, während er die Nachrichten über sich selbst umleitet, die symmetrisch verschlüsselte Kommunikation abhören und dabei den Nachrichteninhalt sowohl lesen als auch unbemerkt verändern. Um einen solchen Man-In-The-Middle-Angriff auszuschließen, müssen die ausgetauschten Nachrichten zusätzlich authentisiert werden, was beispielsweise mittels elektronsicher Unterschriften erfolgen kann.

Ein weiteres bekanntes Protokoll für den sicheren Datenaustausch in einem dezentralen Netzwerk ist das Needham-Schroeder-Protokoll, das Schlüsselaustausch und Authentifikation mit dem Ziel vereint, eine sicher Kommunikation zwischen zwei Partnern in einem dezentralen Netzwerk zu etablieren. Die Grundlage für die Sicherheit dieses Protokolls sind sichere Verschlüsselungsalgorithmen mit beliebigen Schlüsseln, die weder durch Kryptoanalyse noch durch erschöpfende Suche gebrochen werden können, wobei sowohl symmetrische und asymmetrische Verfahren zum Einsatz kommen können.

Bei der symmetrischen Variante des Needham-Schroeder-Protokolls wird vorausgesetzt, dass sowohl A als auch B jeweils einen geheimen Schlüssel mit einem so genannten Authentication-Server besitzen. Damit nun A mit B einen sicheren Datenaustausch durchführen kann, schickt A in einem ersten Schritt eine Nachricht an den Authentication-Server, der in weiterer Folge in die an A zurückgeschickte Antwort zweimal den Sitzungsschlüssel einfügt, und zwar einmal mit dem geheimen Schlüssel von A und einmal mit dem geheimen Schlüssel von B verschlüsselt. In weiterer Folge sendet A den mit dem geheimen Schlüssel von B verschlüsselten Sitzungsschlüssel an B, sodass schlussendlich sowohl A als auch B im Besitz des vom Authentication-Server vergebenen Sitzungsschlüssels sind.

Aus der US 5 999 625 A ist ein Verfahren zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern bekannt, wobei die Transaktion der Nachrichten unter Zwischenschaltung einer Authentifizierungseinrichtung erfolgt, welche die von Anwendern erhaltenen Nachrichten entschlüsselt und wiederum Nachrichten an die Anwender sendet. Die in dieser Schrift beschriebene Lösung basiert auf ein symmetrisches kryptografisches Protokoll,

wobei die zumindest beiden Anwender jeweils den öffentlichen Schlüssel der Authentifizierungseinrichtung benutzen, um die erste und die zweite verschlüsselte Nachricht zu erstellen. Zum Nachweis der Echtheit der Nachrichten wird allenfalls vorgeschlagen, in bekannter Weise, digitale Zertifikate zu verwenden.

Das Zwischenschalten einer Authentifizierungseinrichtung zur Wahrung der Privatsphäre bei einer Transaktion zwischen zumindest zwei Anwendern wird weiters in der WO 2001/001361 A1 erwähnt, wobei diese Lösung auf ein symmetrisches kryptografisches Protokoll basiert.

Gemäß der WO 2003/046685 A2 fordert ein erster Anwender zu Beginn einer Transaktion von einer Authentifizierungseinheit einen einmaligen Autorisierungscode an, der durch Verschlüsselung der Transaktionsparameter gebildet wird. In einer Datenbank der Authentifizierungseinheit werden anschließend in einem Datensatz die Transaktionsparameter und der zugeordnete Autorisierungscode gespeichert. Vor Abschluss der Transaktion muss der zweite Anwender an die Authentifizierungseinheit den zu den Transaktionsparametern passenden Autorisierungscode vorweisen. Zur Überprüfung der Gültigkeit der Transaktion wird überprüft, ob diese mit dem eingangs gespeicherten Datensatz übereinstimmen. Erst bei Übereinstimmung wird dann die Transaktion auch tatsächlich durchgeführt.

Das Problem der bisher bekannten Kryptosysteme liegt also in der direkten Nachrichtenübertragung zwischen den beiden Anwendern. Zwar sind diese Nachrichten verschlüsselt, gelingt es aber einem Angreifer, in den Besitz entweder des geheimen gemeinsamen Schlüssels bei symmetrischen Verfahren oder des Private-Keys bei asymmetrischen Verfahren zu gelangen, ist der Angreifer in der Lage, die übermittelten Nachrichten zu lesen.

Die Erfindung hat es sich daher zur Aufgabe gemacht, ein neuartiges Verfahren zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern anzugeben, mit dem die vorbeschriebenen Nachteile vermieden werden können.

Das erfindungsgemäße Verfahren löst diese Aufgabe durch die Schritte:

a1) Senden einer Nachricht (NA_1) durch einen ersten Anwender (A) an die Authentifizierungseinrichtung (AE),
a2) Erstellen eines Transaktionsidentifikationsdatensatzes (T_{ID}) durch die Authentifizierungseinrichtung (AE),
a3) Senden einer den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NAE_1) durch die Authentifizierungseinrichtung (AE) an den ersten Anwender (A),
a4) Erstellen einer mit einem Schlüssel (SA_2) verschlüsselten, den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NA_2) durch den ersten Anwender (A);
b) Senden der Nachricht (NA_2) an einen zweiten Anwender (B),
c) Erstellen einer die verschlüsselte Nachricht (NA_2) beinhaltenden, mit einem weiteren Schlüssel (SB) verschlüsselten Nachricht (NB_1) durch den zweiten Anwender (B),
d) Senden der Nachricht (NB_1) an die Authentifizierungseinrichtung (AE),
e) Entschlüsseln der Nachricht (NB_1), (NA_2) unter Verwendung der entsprechenden Schlüssel (SB_1), (SA_2) durch die Authentifizierungseinrichtung (AE),
f) Erstellen einer Nachricht (NAE_2) durch die Authentifizierungseinrichtung (AE) unter Bezugnahme auf die in den entschlüsselten Nachrichten (NA_2), (NB_1) enthaltenen Klartexte (A_2), (B_1) und
g) Senden der Nachricht (NAE_2) an den ersten Anwender (A) und/oder den zweiten Anwender (B);

Anders ausgedrückt findet erfindungsgemäß zwischen den beiden Anwender kein Schlüsselaustausch sondern lediglich eine Schlüsselweitergabe statt, sodass keiner der beiden Anwender die Möglichkeit noch die Fähigkeit hat, verschlüsselte Nachrichten des jeweilig anderen Anwenders zu entschlüsseln und zu lesen.

Gemäß einem bevorzugten Ausführungsbeispiel der Erfindung ist vorgesehen, dass die vom ersten Anwender erstellte, verschlüsselte Nachricht einen Transaktionsidentifikationsdatensatz, vorzugsweise eine Transaktionsidentifikationsnummer, umfasst, wobei der Austausch von Transaktionsinformationen auf die direkte Verbindung zwischen Anwender und Authentifizierungseinrichtung limitiert ist.

Das heißt, dass die Entschlüsselung der Daten nur durch die Authentifizierungseinrichtung erfolgen kann, wobei gemäß einem weiteren Ausführungsbeispiel der Erfindung die Authentifizierungseinrichtung den Transaktionsidentifikationsdatensatz erstellt und eine den Transaktionsidentifikationsdatensatz enthaltende Nachricht an den Anwender sendet, der diesen erhaltenen Transaktionsidentifikationsdatensatz in die von ihm an den zweiten Anwender zu sendende verschlüsselte Nachricht integriert.

Gemäß einem weiteren Ausführungsbeispiel der Erfindung ist vorgesehen, dass die Authentifizierungseinrichtung einen Authentifizierungsserver und einen Datenserver aufweist, wobei der Authentifizierungsserver einen der vom ersten Anwender an die Authentifizierungseinrichtung gesandten Nachricht zugeordneten bzw. zuordenbaren Datenbankeintrag auf dem Datenbankserver erstellt, wobei günstigerweise der Transaktionsidentifikationsdatensatz dem Datenbankeintrag eindeutig zugeordnet bzw. zuordenbar ist.

Das Erstellen eines Datenbankeintrages auf einem Datenbankserver und der Zuordnung eines Transaktionsidentifikationsdatensatzes zu dem erstellten Datenbankeintrag ermöglicht es der Authentifizierungseinrichtung die von den Anwendern erhaltenen verschlüsselten Nachrichten nach dem Entschlüsseln einander zuzuordnen. Dafür hat es sich weiters als vorteilhaft herausgestellt, wenn die von der Authentifizierungseinrichtung an den ersten Anwender transferierte Nachricht neben dem Transaktionsidentifikationsdatensatz weitere, vorzugsweise dynamische Transaktionsinformationen beinhaltet.

Obwohl es nicht notwendig ist, die vom ersten Anwender an die Authentifizierungseinrichtung übermittelte Anfrage sowie die den Transaktionsidentifikationsdatensatz beinhaltende Antwort zu verschlüsseln, da ein möglicher Angreifer aufgrund der darin enthaltenen Informationen nicht in der Lage ist, Rückschlüsse auf die später von den Anwendern eingesetzten Schlüssel zu ziehen, kann gemäß einem weiteren Ausführungsbeispiel der Erfindung vorgesehen sein, dass die Nachricht vom ersten Anwender zur Authentifizierungseinrichtung und/oder die Nachricht von der Authentifizierungseinrichtung an den ersten Anwender vor dem Transfer zumindest teilweise verschlüsselt wird (werden).

Im Gegensatz zum Needham-Schroeder-Protokoll sind beim erfindungsgemäßen Verfahren statische Identifikationen der jeweiligen Gegenpartei einem Anwender weder bekannt noch werden diese zwischen den Anwendern ausgetauscht. Die Transaktionsinformationen werden lediglich von der Authentifizierungseinrichtung an den ersten Anwender, von diesem an den zweiten Anwender und vom zweiten Anwender an die Authentifizierungseinrichtung weitergegeben, wobei jeder der Anwender zu den erhaltenen verschlüsselten Informationen eigene Informationen hinzufügt, das Gesamtpaket verschlüsselt und dieses verschlüsselte Gesamtpaket an den nächsten Anwender weitergibt, der gleich verfährt.

Das heißt, der tatsächliche Austausch von Transaktionsinformationen ist auf die direkte Verbindung vom Anwender zur Authentifizierungseinrichtung limitiert, sodass die Entschlüsselung der Daten nur durch die Authentifizierungseinrichtung geschehen kann. Dieses neuartige Prinzip der „in sich" verschlüsselten Datenübertragung erlaubt eine sichere Abwicklung des Datentransfers zwischen zwei Anwendern in einem Netzwerk unabhängig davon, ob es sich dabei um das Internet, ein Intranet, ein Xtranet, ein WAN oder ein LAN oder ähnlichen Verbindungsarten zwischen zwei Anwendern, die gesicherte Daten übertragen möchten, handelt.

Gemäß einem weiteren Ausführungsbeispiel der Erfindung, ist vorgesehen, dass die Authentifi-

zierungseinrichtung die erhaltenen Nachrichten unter Verwendung der entsprechenden Schlüssel entschlüsselt und die in den entschlüsselten Nachrichten enthaltenen Klartexte vergleicht, abgleicht oder kombiniert, bevor sie eine auf das Ergebnis des Vergleichens, Abgleichens und Kombinierens der Klartexte bezugnehmende Nachricht erstellt.

Dadurch, dass das Entschlüsseln, Vergleichen, Abgleichen und Kombinieren ausschließlich durch die Authentifizierungseinrichtung erfolgt, wird durch das erfindungsgemäße Verfahren eine gegenüber dem Stand der Technik erhöhte Sicherheit bei Datentransfers in Netzwerken erreicht.

Dabei sieht ein weiteres Ausführungsbeispiel der Erfindung vor, dass die Authentifizierungseinrichtung nach dem Vergleichen, Abgleichen oder Kombinieren der in den entschlüsselten Nachrichten enthaltenen Klartexte eine auf das Ergebnis des Vergleichens, Abgleichens oder Kombinierens bezugnehmende Aktion setzt und danach eine auf die gesetzte Aktion bezugnehmende Nachricht erstellt.

Weiters ist es durchaus möglich, den Anwendern dieselbe, jedoch mit verschiedenen Schlüsseln verschlüsselte Nachricht über die gesetzte Aktion zu übermitteln. Eine erhöhte Sicherheit kann gemäß einem weiteren Ausführungsbeispiel jedoch dann erreicht werden, wenn die Authentifizierungseinrichtung eine für den ersten Anwender bestimmte Nachricht und eine für den zweiten Anwender bestimmte Nachricht erstellt und an die jeweiligen Anwender versendet, sodass ein Angreifer, der in Besitz des gemeinsamen geheimen Schlüssels zwischen der Authentifizierungseinrichtung und einem Anwender ist, lediglich die für diesen Anwender bestimmte Information lesen kann, aufgrund dieser Information aber keine Rückschlüsse auf die zwischen den beiden Anwendern transferierten Daten ziehen kann.

Wenngleich das Grundprinzip des neuartigen Verfahrens auf keine spezielle Übertragungsart beschränkt ist, sieht ein bevorzugtes Ausführungsbeispiel der Erfindung vor, dass der Transfer der Nachrichten über ein Netzwerk, vorzugsweise über das Internet, erfolgt.

Wie an sich von Kryptosystemen bekannt, beinhaltet dabei wenigstens eine der verschlüsselten Nachrichten einen Klartext und einen Transaktionsidentifikationsdatensatz sowie bevorzugterweise weiters verschlüsselte, vorzugsweise dynamische Transaktionsinformationen.

Um zu verhindern, dass ein möglicher Angreifer die transferierten Daten in einfacher Weise lesen kann, sieht ein Ausführungsbeispiel der Erfindung vor, dass wenigstens ein Anwender wenigstens einen geheimen Schlüssel mit der Authentifizierungseinrichtung besitzt, wobei es sich als günstig herausgestellt hat, wenn jeder Anwender jeweils wenigstens einen geheimen Schlüssel mit der Authentifizierungseinrichtung besitzt. Ist dies der Fall, hat es sich als günstig herausgestellt, wenn die Nachrichten gemäß einem symmetrischen kryptografischen Protokoll transferiert werden.

Mit dem erfindungsgemäßen Verfahren wird also ein Verfahren bereitgestellt, dessen Einsatz zu einem absolut sicheren Kryptosystem führt, das heißt, die transferierten Daten beinhalten zu keinem Zeitpunkt genügend Informationen, um daraus Klartext oder Schlüssel ableiten zu können. Damit stellt das erfindungsgemäße Verfahren neben dem bisher einzigen als sicher geltenden Kryptosystem, dem sogenannten One-Time-Pad, ein zweites absolut sicheres Kryptosystem zur Verfügung, welche das Kerckhoffsche-Prinzip, gemäß dem die Sicherheit eines Kryptosystems nicht von der Geheimhaltung des Algorithmus abhängen darf sondern sich nur auf die Geheimhaltung des Schlüssels gründet, in idealer Weise erfüllt.

Um die grundlegenden Voraussetzungen zur Wahrung der Sicherheit des erfindungsgemäßen Verfahrens, die da lauten, der Einmalschlüssel muss geheim bleiben, muss unvorhersagbar zufällig sein und darf nur einmal verwendet werden, erfüllen zu können, sieht ein weiteres Ausführungsbeispiel der Erfindung vor, dass der/die Schlüssel zwischen dem(den) Anwender(n)

und der Authentifizierungseinrichtung mittels eines mobilen Datenträgers, auf dem der Schlüssel gespeichert ist und/oder der zum Generieren des/der Schlüssel ausgebildet ist, verteilt wird/werden, wobei jedem Anwender jeweils ein eigener Datenträger zugeordnet bzw. zuordenbar ist. Der einem Anwender zugeordnete mobile Datenträger ist dabei zum Generieren mehrerer vorzugsweise einmaliger Schlüssel ausgebildet ist, wobei der jeweilige Anwender alle von dem ihm zugeordneten Datenträger generierten Schlüssel gemeinsam mit der Authentifizierungseinrichtung besitzt.

Das erfindungsgemäße Verfahren kann beispielsweise zur Sicherstellung von Kompensationen für geleistete Dienstleistungen und Warenlieferungen, einem sogenannten Clearing - Prozess, verwendet werden und bedient sich dabei bereits allgemein genutzter und erprobter Verschlüsselungsmethoden. Im Nachfolgend beschriebenen Beispiel findet der Vertragsabschluss zwischen Lieferanten und Kunde außerhalb der Kontrolle des neuartigen Verfahrens statt, weshalb auf diesen Schritt nicht näher eingegangen wird.

Der Clearing-Prozess lässt sich im Wesentlichen in vier Teilschritte strukturieren, nämlich in einen ersten Schritt, bei dem der Lieferant eine Forderung gegenüber einem Kunden bei der Authentifizierungseinrichtung mit Angabe der Fälligkeit hinterlegt. Diese Forderung beinhaltet die maßgeblichen Elemente der Kompensationsforderung als Lieferung in Einheiten. Im zweiten Schritt bestätigt der Kunde die Forderung bezüglich der Lieferung der Einheiten zu einem spezifischen Zeitpunkt, der sofort aber auch ein definites Datum der Zukunft sein kann. Im dritten Schritt bestätigt dann die Authentifizierungseinrichtung das Matching der Forderung und blockiert die Einheiten für den Transfer bis zum vereinbarten Zeitpunkt, woraufhin in Schritt vier die Abwicklung, respektive das Clearing der Forderung zum vereinbarten Zeitpunkt erfolgt.

Neben dem erfindungsgemäßen Verfahren soll weiters eine hardwaremäßige Verschlüsselungseinrichtung, die sich insbesondere zur Verwendung im erfindungsgemäßen Verfahren eignet, angegeben werden.

Im Unterschied zu den bisher bekannten hardewaremäßigen Verschlüsselungseinrichtungen, beispielsweise einer Smart Card, ist die erfindungsgemäße Verschlüsselungseinrichtung in der Lage spezifische Algorithmen zu implementieren, sodass der Schlüssel der jeweils je Anwender aus einem mit einem dynamischen Schlüssel ergänzten Basisschlüssel besteht, pro Verschlüsselungsvorgang neu erzeugt wird und auf diese Weise einmalig ist. Zu diesem Zweck sieht die Erfindung vor, dass die hardwaremäßige Verschlüsselungseinrichtung von einem mobilen Datenträger, der eine Speichereinheit, eine Recheneinheit zum Erzeugen wenigstens eines vorzugsweise einmaligen Schlüssels und eine Schnittstelle, vorzugsweise eine USB-Schnittstelle, aufweist, gebildet ist.

Um eine unerlaubte Verwendung der Verschlüsselungseinrichtung zu verhindern, kann weiters vorgesehen sein, dass sie eine biometrische Zugriffskontrolleinrichtung aufweist, wobei ein bevorzugtes Ausführungsbeispiel der Erfindung vorsieht, dass die biometrische Zugriffskontrolleinrichtung einen Sensor zum Erkennen eines Fingerabdruckes aufweist.

Neben der Verwendung der biometrischen Zugriffskontrollvorrichtung für die Verifizierung des Benutzers der Verschlüsselungseinrichtung wäre es auch denkbar, das von der biometrischen Zugriffskontrollvorrichtung verifizierte biometrische Merkmal des Benutzers zur Erzeugung des Schlüssels zu verwenden.

Ein weiterer Aspekt der Erfindung liegt in der Verwendung eines USB-Sticks, vorzugsweise mit Fingerabdruckerkennungsfunktion, als Verschlüsselungseinrichtung in der Kryptografie.

Weitere Vorteile und Einzelheiten der Erfindung werden anhand der nachfolgenden Figurenbeschreibung unter Bezugnahme auf die in der Zeichnung dargestellten Ausführungsbeispiele näher erläutert. Darin zeigt

Fig. 1a und 1b im Prinzip die Verfahrensschritte eines ersten Ausführungsbeispieles der Erfindung,
Fig. 2 den Ablauf des Ausführungsbeispieles gemäß Fig. 1 im Detail und
Fig. 3 eine Prinzipskizze einer erfindungsgemäßen Verschlüsselungseinrichtung.

Anhand der Fig. 1 und 1b wird nachfolgend das Grundprinzip der verschlüsselten Datenübertragung beschrieben, welches auf der Grundlage beruht, dass die statischen Identifikationen der Anwender A, B dem jeweiligen anderen Anwender weder bekannt sind noch direkt zwischen den beiden Anwendern A und B übertragen werden. Beim beschriebenen Ausführungsbeispiel werden alle Nachrichten verschlüsselt transferiert.

Der Datentransfer wird vom Anwender A initiiert, der im Schritt 1 eine Nachricht NA_1, die einen mit dem Schlüssel SA_1 verschlüsselten Klartext A_1 umfasst, an die Authentifizierungseinrichtung AE sendet. Als Antwort erhält der Anwender A im Schritt 2 von der Authentifizierungseinrichtung AE eine Nachricht NAE_1, die einen Transaktionsidentifikationsdatensatz T_{ID} sowie mit dem Schlüssel SAE verschlüsselte Transaktionsinformationen T_{Inf} beinhaltet. In weiterer Folge ergänzt der Anwender A die erhaltene Nachricht NAE_1 mit eigenen Informationen A_2 zur Transaktion und verschlüsselt das Gesamtpaket mit dem Schlüssel SA_2 und erzeugt auf diese Weise eine Nachricht NA_2. Diese Nachricht NA_2 sendet er im Schritt 3 an den Anwender B.

Der Anwender B ergänzt seinerseits die erhaltene Nachricht NA_2 mit eigenen Informationen B_1 zur Transaktion, verschlüsselt das Gesamtpaket mit seinem Schlüssel SB_1 und erzeugt auf diese Weise die Nachricht NB_1, die er dann im Schritt 4 an die Authentifizierungseinrichtung AE sendet.

Die Authentifizierungseinrichtung AE entschlüsselt die erhaltenen Nachrichten, vergleicht die beinhalteten Informationen, die unabhängig durch den Anwender A und den Anwender B mittransferiert wurden, d.h. die Authentifizierungseinrichtung AE nimmt das so genannte Matching vor und erstellt auf Basis des Matching-Ergebnisses für den Anwender A eine Nachricht NAE_2, die einen mit dem Schlüssel SA_3 verschlüsselten Klartext E_A beinhaltet, und für den Anwender B eine Nachricht NAE_2', die einen mit dem Schlüssel SB_2 verschlüsselten Klartext E_B beinhaltet und versendet diese beiden Nachrichten gemäß Schritt 5, 5' an die jeweiligen Anwender A und B.

Die Datensicherung und der Datenschutz der übermittelten Nachrichten werden über an sich bekannte Verschlüsselungsmethoden gewährleistet. Sollten die aktuell eingesetzten RSA-Methoden nicht mehr genügen bzw. werden neuere Technologien, mit denen die Sicherheit erhöht werden kann, bekannt, ist das Erneuern bzw. Anpassen der Prozeduren und Algorithmen bei den Anmeldern ohne Austausch irgendwelcher Hardware möglich.

Die Inhalte der Nachrichten, die während einer Transaktion ausgetauscht werden müssen, werden durch einen zuverlässigen Check-Summen-Mechanismus verifiziert. Dazu verwendet das erfindungsgemäße Verfahren einen SHA (Secure Hash Algorithm) mit der Kollisionswahrscheinlichkeit von ca. $1/10^{80}$. Weiters ist jede Datei, die während eines Transfervorganges ausgetauscht wird, durch den jeweiligen Absender signiert.

Wesentlich dabei ist, dass die eigentliche Information des Datentransfers nie direkt zwischen den beiden Anwendern A und B ausgetauscht wird. Das heißt, die eigentliche Information fließt immer über die Authentifizierungseinrichtung, die die Information abgleicht und das Resultat des Abgleichs den beiden Anwendern A, B bestätigt. Daraus folgt, dass die Anwender A, B weder die Möglichkeit noch die Fähigkeit haben, die Information des jeweiligen anderen Anwenders A, B zu entschlüsseln, da ja zwischen den Anwendern A, B kein Schlüsselaustausch sondern lediglich eine verschlüsselte Schlüsselweitergabe stattfindet.

Die eigentliche Kommunikation beim Nachrichtentransfer basiert auf XML-Datenaustausch über

TCP/IP, wobei die Kommunikation zwischen den Anwendern über einen sogenannten Quired Secure Channel, beispielsweise HTTPS, geführt wird.

Die Sicherheit, dass die Schlüssel, die die Anwender mit der Authentifizierungseinrichtung gemeinsam besitzen, tatsächlich geheim und einmalig sind, wird über die hardwaremäßige Verschlüsselungseinrichtung, auf die weiter unten näher eingegangen wird, gewährleistet. Diese Verschlüsselungseinrichtung kann beispielsweise den beiden Anwendern A, B vom Betreiber der Authentifizierungseinrichtung zur Verfügung gestellt werden. Zusätzlich sollte sichergestellt werden, dass die hardwaremäßige Verschlüsselungseinrichtung eines Anwenders keine direkte Kommunikationsanbindung zum Netzwerk des jeweilig anderen Anwenders besitzt.

In Fig. 3 ist die für das erfindungsgemäße Verfahren konzipierte hardwaremäßige Verschlüsselungseinrichtung 6 in einer Prinzipskizze dargestellt. Mit der Verschlüsselungseinrichtung 6 erstellt der Anwender A, B die zu übermittelnde Nachricht, indem er die für den Datentransfer notwendigen Informationen in einen In-Puffer 12 stellt, worauf er das verschlüsselte Resultat im Out-Puffer 13 erhält. Wichtig dabei ist, dass der Benutzer der Verschlüsselungseinrichtung 6 keinen Zugriff auf Daten und Prozesse, die in der Verschlüsselungseinrichtung 6 ablaufen, hat. So kann beispielsweise als weiteres Sicherheitsmerkmal vorgesehen sein, dass jeder versuchte Eingriff bzw. Zugriff auf den geschützten Bereich 11, der sich in der Fig. 3 rechts von der strichpunktierten Linie befindet, die Zerstörung sämtlicher Informationen zur Folge hat.

Die Verschlüsselungseinrichtung 6 verfügt neben dem geschützten Bereich 11 über eine Schnittstelle 9, die beim gezeigten Ausführungsbeispiel als USB-Schnittstelle ausgebildet ist. Innerhalb des geschützten Bereiches 11 befinden sich eine Speichereinheit 7, ein Prozessor 8 und eine biometrische Zugriffskontrolleinrichtung 10. Die Verschlüsselungseinrichtung 6 ist in der Lage spezifische Algorithmen über in der Speichereinheit 7 abgelegte Software zu implementieren und mittels des Prozessors 8 die für den Verschlüsselungsprozess notwendigen Nummern zu erstellen.

Die Verschlüsselungseinrichtung 6 erscheint im angeschlossen System, das beispielsweise von einem PC gebildet wird, als Wechseldatenträger, wobei der in der Schnittstelle 9 der Verschlüsselungseinrichtung 6 angeordnete In-Puffer 12 und der Out-Puffer 13 als Datenordner sichtbar sind. Der Austausch von Daten mit der Verschlüsselungseinrichtung 6 wird über Dateiaustausch in die entsprechenden Ordner gewährleistet. So werden die für den Datentransfer notwendigen Informationen in MXL-Dateien befüllt, die zum Verschlüsseln auf den In-Puffer 12 kopiert werden.

Darüber hinaus kann die Verschlüsselungseinrichtung 6 im Weiteren über einen einfachen Update-Mechanismus verfügen, der es erlaubt, neue bzw. geänderte Software einzuspielen und auf diese Weise die Schlüssel neu bzw. neue Schlüssel zu berechnen.

Um einem Missbrauch der Verschlüsselungseinrichtung 6 vorzubeugen, ist der Fingerprint, der je Anwender spezifisch ist, auf der Verschlüsselungseinrichtung 6 hinterlegt und nur in verschlüsselter Form verfügbar. Als Teil der versendeten Nachrichten wird der Fingerprint bei jeder Verschlüsselung zugefügt, respektive bei jeder Entschlüsselung überprüft.

Im geschützten Bereich 11 der Verschlüsselungseinrichtung 6 befindet sich die Software, die für die Verschlüsselung, die Berechnung des HASH und die Identifizierung des Fingerabdruckes notwendig ist. Die Freigabe des geschützten Bereiches 11 erfolgt über einen Request-Replay-Mechanismus, der durch den jeweiligen Anwender A, B aufgerufen wird. Damit kann die Eingabe eines persönlichen PIN's verbunden sein, durch den die Software erst in Funktion treten kann. Dieser Mechanismus ist unabhängig von der I/O-Funktion der Verschlüsselungseinrichtung 6 selbst.

Weiters befinden sich in diesem geschützten Bereich 11 die notwendigen Schlüssel für den sicheren Datentransfer sowie der Aktivierungsmechanismus für die Verschlüsselungsprogramme, der beispielsweise als PIN-Check ablaufen kann.

Das generelle Format der Nachrichten, die mit der Verschlüsselungseinrichtung 6 erstellt werden, bildet sich aus einer Anwender-ID, des Text-Strings der Informationen, einer Checksumme über die Information und der Signatur des Anwenders, wobei die Kommunikation zwischen den Anwendern A, B und der Authentifizierungseinrichtung AE generell auf Web-Services, beispielsweise Soap, basiert.

Die Informationen werden über XML-Formate ausgetauscht und sind so für die Anwender gleichermaßen interpretierbar. Die Übermittlung der Informationen erfolgt in Nachrichten in Form von Datenpaketen, die jeweils mit einem Hash-Key und dem Fingerprint, der die Signatur darstellt, versehen sind. Der Nachrichtenaustausch geschieht dabei in verschlüsselter Form zwischen den Anwendern.

Nachfolgend wird unter Bezugnahme auf die Fig. 2 ein Nachrichtentransfer gemäß der Erfindung im Detail beschrieben.

Im Schritt I erstellt der Anwender A den Klartext A_1 den er in Schritt II mit dem Schlüssel SA_1 verschlüsselt und auf diese Weise die Nachricht NA_1 erzeugt. Die Erzeugung der Nachricht NA_1 erfolgt wie vorbeschrieben mittels der Verschlüsselungseinrichtung 6, indem er die notwendigen Informationen in den Eingangspuffer/In-Puffer 12 der Verschlüsselungseinrichtung 6 schreibt. Als Resultat erhält er die verschlüsselte Nachricht NA_1. Gemäß Verfahrensschritt a1) sendet dann der Anwender A die verschlüsselte Nachricht NA_1 an die Authentifizierungseinrichtung AE, beispielsweise über einen „Transaction-Start-Request".

Der Authentifikationsserver AS der Authentifizierungseinrichtung AE empfängt in Schritt III die Nachricht NA_1, entschlüsselt diese gemäß Schritt IV und beginnt die Transaktionssequenz, indem der Authentifikationsserver AS einen neuen Datenbankeintrag DB auf dem Datenserver DS der Authentifizierungseinrichtung AE erstellt (Schritt V) und in Schritt VI gleichzeitig einen für diese Transaktion eindeutigen Transaktionsidentifikationsdatensatz T_{ID}, der dem Datenbankeintrag DB eindeutig zuordenbar ist, generiert (gemäß Verfahrensschritt a2)).

In Schritt VII generiert der Authentifikationsserver AS eine Nachricht NAE_1, die neben dem Transaktionsidentifikationsdatensatz T_{ID} weitere mit dem Schlüssel SAE verschlüsselte Transaktionsinformationen T_{Inf} beinhaltet.

Gemäß Verfahrensschritt a3) erhält der Anwender A in Schritt VIII diese Nachricht NAE_1, wobei die verschlüsselten Transaktionsinformationen T_{Inf} für den Anwender A nicht lesbar sind. In Schritt IX ergänzt der Anwender A die erhaltene Nachricht in NAE_1 mit eigenen Daten A_2 für die Transaktion und verschlüsselt dieses Gesamtpaket gemäß Schritt X mit dem Schlüssel SA_2 und erzeugt auf diese Weise die Nachricht NA_2. Gemäß Verfahrensschritt b) übergibt der Anwender A die Nachricht NA_2 an den Anwender B, der diese Nachricht gemäß Schritt XI empfängt.

Der Anwender B verfügt zwar auch über eine Verschlüsselungseinrichtung 6, da jede Verschlüsselungseinrichtung 6 für sich jedoch einmalig ist, ist es dem Anwender B nicht möglich, die vom Anwender A erhaltene Nachricht NA_2 mit seiner Verschlüsselungseinrichtung 6 zu entschlüsseln.

Analog zu Schritt IX ergänzt der Anwender B gemäß Schritt XII die erhaltene Nachricht NA_2 mit eigenen Informationen B_1 zur Transaktion und übergibt das Gesamtpaket an seine Verschlüsselungseinrichtung 6 weiter. Als Resultat erhält der Anwender B im Schritt XIII ein mit dem Schlüssel SB_1 verschlüsselte Nachricht NB_1 (Verfahrensschritt c)).

In weiterer Folge übermittelt der Anwender B gemäß Verfahrensschritt d) die Nachricht NB_1 an den Authentifizierungsserver AS mittels einer „Transaction-Confirmation". Der Authentifizierungsserver AS empfängt gemäß Schritt XIV die Nachricht NB_1 und ist durch die Anwendung der Schlüssel SA, SB, die die Authentifizierungseinrichtung AE gemeinsam mit den Anwendern A, B besitzt, in der Lage, die erhaltene Nachricht NB_1 stufenweise zu entschlüsseln (Schritt XV).

In weiterer Folge ist es dem Authentifizierungsserver AS gemäß Verfahrensschritte e1) und e2) in Verbindung mit dem Datenserver DS möglich, die Informationen, die während des Datentransfers von den Anwendern A, B unabhängig mitgegeben wurden, miteinander zu vergleichen und ein so genanntes Matching vorzunehmen (Schritt XVI).

Beim gezeigten Ausführungsbeispiel setzt der Authentifizierungsserver AS nach dem Matching gemäß Verfahrensschritt e3) eine auf das Ergebnis des Matching Bezugnehmende Aktion E (Schritt XVII).

Gemäß Verfahrensschritt f) erstellt der Authentifizierungsserver AS in weiterer Folge in den Schritten XVIII, XVIII' eine auf die gesetzte Aktion E Bezugnehmende Nachricht NAE_2 für den Anwender A und eine Nachricht NAE_2' für den Anwender B.

In Verbindung mit dem Datenserver DS nutzt der Authentifizierungsserver nun das umgekehrte Verfahren und gibt gemäß Verfahrensschritt g dem Anwender A und dem Anwender B verschlüsselt jeweils individuelle Transaktionsbestätigungen zurück, die von den jeweiligen Anwendern A, B gemäß Schritt XX, XX' mit den jeweiligen Schlüsseln entschlüsselt werden.

Das beschriebene Ausführungsbeispiel eines Verfahrens zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern sowie das dargestellte Ausführungsbeispiel einer Verschlüsselungseinrichtung sind selbstverständlich nicht im einschränkenden Sinne zu verstehen sondern eben nur einzelne Beispiele von zahlreichen Möglichkeiten, den Erfindungsgedanken zu realisieren.

So wäre es beispielsweise auch denkbar, dass nur einer der beiden Anwender einen geheimen gemeinsamen Schlüssel mit der Authentifizierungseinrichtung besitzt, während der zweite Anwender mit der Authentifizierungseinrichtung eine Public-Key Verschlüsselung nutzt. Erfindungswesentlich ist jedenfalls der Umstand, dass zwischen den beiden Anwendern keine statischen Identifikationsdaten ausgetauscht werden, d.h. beim erfindungsgemäßen Verfahren erfolgt zwischen den beiden Anwendern kein Schlüsselaustausch sondern lediglich eine verschlüsselte Schlüsselweitergabe, wobei jeder Teilnehmer einer Transaktion die erhaltenen verschlüsselten Datenpakete mit seinem eigenen Schlüssel zusätzlich verschlüsselt und weitergibt, und nur die Authentifizierungseinrichtung in der Lage ist, das Datenpaket stufenweise zu entschlüsseln.

Patentansprüche:

1. Verfahren zum Transferieren von verschlüsselten Nachrichten zwischen wenigstens zwei Anwendern, insbesondere kryptografisches Protokoll, wobei die Transaktion der Nachrichten unter Zwischenschaltung einer Authentifizierungseinrichtung erfolgt, welche die von den Anwendern erhaltenen Nachrichten entschlüsselt und wiederum insbesondere verschlüsselte Nachrichten an die Anwender sendet und folgende Schritte umfasst:
   a1) Senden einer Nachricht (NA_1) durch einen ersten Anwender (A) an die Authentifizierungseinrichtung (AE),
   a2) Erstellen eines Transaktionsidentifikationsdatensatzes (T_{ID}) durch die Authentifizierungseinrichtung (AE),
   a3) Senden einer den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NAE_1) durch die Authentifizierungseinrichtung (AE) an den ersten Anwender (A),

a4) Erstellen einer mit einem Schlüssel (SA_2) verschlüsselten, den Transaktionsidentifikationsdatensatzes (T_{ID}) enthaltenden Nachricht (NA_2) durch den ersten Anwender (A);
b) Senden der Nachricht (NA_2) an einen zweiten Anwender (B),
c) Erstellen einer die verschlüsselte Nachricht (NA_2) beinhaltenden, mit einem weiteren Schlüssel (SB) verschlüsselten Nachricht (NB_1) durch den zweiten Anwender (B),
d) Senden der Nachricht (NB_1) an die Authentifizierungseinrichtung (AE),
e) Entschlüsseln der Nachricht (NB_1), (NA_2) unter Verwendung der entsprechenden Schlüssel (SB_1), (SA_2) durch die Authentifizierungseinrichtung (AE),
f) Erstellen einer Nachricht (NAE_2) durch die Authentifizierungseinrichtung (AE) unter Bezugnahme auf die in den entschlüsselten Nachrichten (NA_2), (NB_1) enthaltenen Klartexte (A_2), (B_1) und
g) Senden der Nachricht (NAE_2) an den ersten Anwender (A) und/oder den zweiten Anwender (B).

2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, dass die vom ersten Anwender (A) erstellte, verschlüsselte Nachricht (NA_2) einen Transaktionsidentifikationsdatensatz (T_{ID}), vorzugsweise eine Transaktionsidentifikationsnummer, umfasst.

3. Verfahren nach Anspruch 2, *dadurch gekennzeichnet*, dass die von der Authentifizierungseinrichtung (AE) an den ersten Anwender (A) transferierte Nachricht (NAE_1) neben dem Transaktionsidentifikationsdatensatz (T_{ID}) mit einem Schlüssel (SAE) verschlüsselte, vorzugsweise dynamische Transaktionsinformationen (T_{Inf}) beinhaltet.

4. Verfahren nach Anspruch 2 oder 3, *dadurch gekennzeichnet*, dass die Nachricht (NA_1,) vom ersten Anwender (A) zur Authentifizierungseinrichtung (AE) und/oder die Nachricht (NAE_1) von der Authentifizierungseinrichtung (AE) an den ersten Anwender (A) vor dem Transfer zumindest teilweise verschlüsselt wird (werden).

5. Verfahren nach einem der Ansprüche 2 bis 4, *dadurch gekennzeichnet*, dass die Authentifizierungseinrichtung (AE) einen Authentifizierungsserver (AS) und einen Datenserver (DS) aufweist, wobei der Authentifizierungsserver (AS) einen der vom ersten Anwender (A) an die Authentifizierungseinrichtung (AE) gesandten Nachricht (NA_1) zugeordneten bzw. zuordenbaren Datenbankeintrag (DB) auf dem Datenbankserver (DS) erstellt.

6. Verfahren nach Anspruch 5, *dadurch gekennzeichnet*, dass der Transaktionsidentifikationsdatensatz (T_{ID}) dem Datenbankeintrag (DB) eindeutig zugeordnet bzw. zuordenbar ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, *gekennzeichnet durch* die Schritte:
e1) Entschlüsseln der Nachrichten (NB_1), (NA_2) unter Verwendung der entsprechenden Schlüssel (SB_1), (SA_2) durch die Authentifizierungseinrichtung (AE),
e2) Matching der in den entschlüsselten Nachrichten (NA_2), (NB_1,) enthaltenen Klartexte (A_2), (B_1) und
f) Erstellen einer auf das Ergebnis des Vergleichens, Abgleichens oder Kombinierens der Klartexte (A_2), (B_1) Bezugnehmenden Nachricht (NAE_2) durch die Authentifizierungseinrichtung (AE);

8. Verfahren nach einem der Ansprüche 1 bis 7, *gekennzeichnet durch* die Schritte:
e1) Entschlüsseln der Nachrichten (NB_1), (NA_2) unter Verwendung der entsprechenden Schlüssel (SB_1), (SA_2) durch die Authentifizierungseinrichtung (AE),
e2) Matching der in den entschlüsselten Nachrichten (NA_2), (NB_1) enthaltenen Klartexte (A_2), (B_1),
e3) Setzen einer auf das Ergebnis des Vergleichens, Abgleichens oder Kombinierens Bezugnehmenden Aktion (E) und
f) Erstellen einer auf die gesetzte Aktion (E) Bezugnehmenden Nachricht (NAE_2) durch die Authentifizierungseinrichtung (AE);

9. Verfahren nach einem der Ansprüche 1 bis 8, *gekennzeichnet durch* die Schritte:
   f) Erstellen einer für den ersten Anwender (A) bestimmten Nachricht (NAE_2) und einer für den zweiten Anwender (B) bestimmten Nachricht (NAE_2') durch die Authentifizierungseinrichtung (AE) unter Bezugnahme auf in den erhaltenen und entschlüsselten Nachrichten (NA_2), (NB_1) enthaltenden Klartexten (A_2), (B_1) und
   g) Senden der Nachricht (NAE_2) an den ersten Anwender (A) und der Nachricht (NAE_2') den zweiten Anwender (B);

10. Verfahren nach einem der Ansprüche 1 bis 9, *dadurch gekennzeichnet*, dass die Nachricht(en) (NAE_2), (NAE_2') vor dem Versenden von der Authentifizierungseinrichtung (AE) mit den den jeweiligen Anwendern (A, B) zugeordneten Schlüsseln (SB_2), (SA_3) verschlüsselt werden.

11. Verfahren nach einem der Ansprüche 1 bis 10, *dadurch gekennzeichnet*, dass der Transfer der Nachrichten (NA_1, NA_2, NB_1, NAE_1, NAE_2, NAE_2') über ein Netzwerk, vorzugsweise über das Internet, erfolgt.

12. Verfahren nach einem der Ansprüche 1 bis 11, *dadurch gekennzeichnet*, dass wenigstens eine der verschlüsselten Nachrichten (NA_2), (NB_1), (NA_2) einen Klartext (A), (B) und einen Transaktionsidentifikationsdatensatz (T_{ID}) beinhaltet.

13. Verfahren nach Anspruch 12, *dadurch gekennzeichnet*, dass wenigstens eine der verschlüsselten Nachrichten (NA_2), (NB_1), (NA_2) weiters verschlüsselte, vorzugsweise dynamische Transaktionsinformationen (T_{Inf}) beinhaltet.

14. Verfahren nach einem der Ansprüche 1 bis 13, *dadurch gekennzeichnet*, dass wenigstens ein Anwender (A, B) wenigstens einen geheimen Schlüssel (SA, SB) mit der Authentifizierungseinrichtung (AE) besitzt.

15. Verfahren nach Anspruch 14, *dadurch gekennzeichnet*, dass jeder Anwender (A, B) jeweils wenigstens einen geheimen Schlüssel (SA, SB) mit der Authentifizierungseinrichtung (AE) besitzt.

16. Verfahren nach Anspruch 15, *dadurch gekennzeichnet*, dass die Nachrichten (NA_1, NA_2, NB_1, NAE_1, NAE_2, NAE_2') gemäß einem symmetrischen kryptografischen Protokoll transferiert werden.

17. Verfahren nach einem der Ansprüche 14 bis 16, *dadurch gekennzeichnet*, dass der/die Schlüssel (SA, SB) zwischen dem(den) Anwender(n) (A, B) und der Authentifizierungseinrichtung (AE) mittels eines mobilen Datenträgers (6), auf dem der Schlüssel (SA, SB) gespeichert ist und/oder der zum Generieren des Schlüssel (SA, SB) ausgebildet ist, verteilt wird/werden, wobei jedem Anwender (A, B) jeweils ein eigener Datenträger zugeordnet bzw. zuordenbar ist.

18. Verfahren nach Anspruch 17, *dadurch gekennzeichnet*, dass der einem Anwender (A, B) zugeordnete mobile Datenträger (6) zum Generieren mehrerer vorzugsweise einmaliger Schlüssel (SA_1, SA_2; SB_1, SB_2) ausgebildet ist, wobei der jeweilige erste Anwender (A, B) alle von dem ihm zugeordneten Datenträger (1) generierten Schlüssel (SA_1, SA_2; SB_1, SB_2) gemeinsam mit der Authentifizierungseinrichtung (AE) besitzt.

19. Verwendung einer hardwaremäßigen Verschlüsselungseinrichtung in einem Verfahren nach einem der Ansprüche 1 bis 18, *dadurch gekennzeichnet*, dass die Verschlüsselungseinrichtung von einem mobilen Datenträger (6), der eine Speichereinheit (7), eine Recheneinheit (8) zum Erzeugen wenigstens eines vorzugsweise einmaligen Schlüssels (SA, SB) und eine Schnittstelle (9), vorzugsweise eine USB-Schnittstelle, aufweist, gebildet ist.

20. Verschlüsselungseinrichtung nach Anspruch 19, *dadurch gekennzeichnet*, dass sie eine biometrische Zugriffskontrolleinrichtung (10) aufweist.

21. Verschlüsselungsvorrichtung nach Anspruch 20, *dadurch gekennzeichnet*, dass die biometrische Zugriffskontrolleinrichtung (10) einen Sensor zum Erkennen eines Fingerabdruckes aufweist.

22. Verwendung eines USB-Sticks als Verschlüsselungseinrichtung in einem Verfahren nach einem der Ansprüche 1 bis 21.

23. USB-Stick nach Anspruch 22, *dadurch gekennzeichnet*, dass der USB-Stick eine Fingerabdruck-Erkennungs-Funktion aufweist.

Hiezu 2 Blatt Zeichnungen

Int. Cl.[8]: ***G07F 7/10*** (2006.01)
G06Q 20/00 (2006.01)
G06Q 30/00 (2006.01)
H04L 9/32 (2006.01)

Fig. 1a

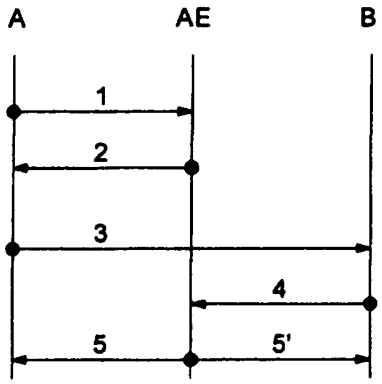
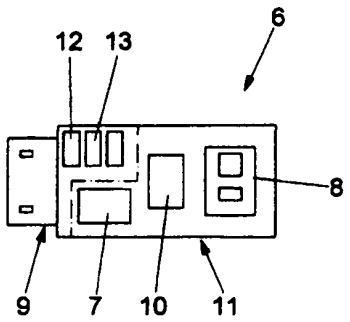


Fig. 1b

(1) A → AE: $NA_1 = (\{A_1\}_{SA_1})$
(2) AE → A: $NAE = (T_{ID}, \{Tinf\}_{SAE})$
(3) A → B: $NA_2 = (\{NAE_1, A_2\}_{SA_2}) = (\{T_{ID}, \{T_{inf}\}_{SAE}, A_2\}_{SA_2})$
(4) B → AE: $NB_1 = (\{NA_2, B_1\}_{SB_1}) = (\{\{T_{ID}, \{T_{inf}\}_{SAE}, A_2\}_{SA_2}, B_1\}_{SB_1})$
(5) AE → A: $NAE_2 = \{E_A\}_{SA_3}$
(5') AE → B: $NAE_2 = \{E_B\}_{SB_2}$

Fig. 3



Int. Cl.[8]: ***G07F 7/10*** (2006.01)
G06Q 20/00 (2006.01)
G06Q 30/00 (2006.01)
H04L 9/32 (2006.01)

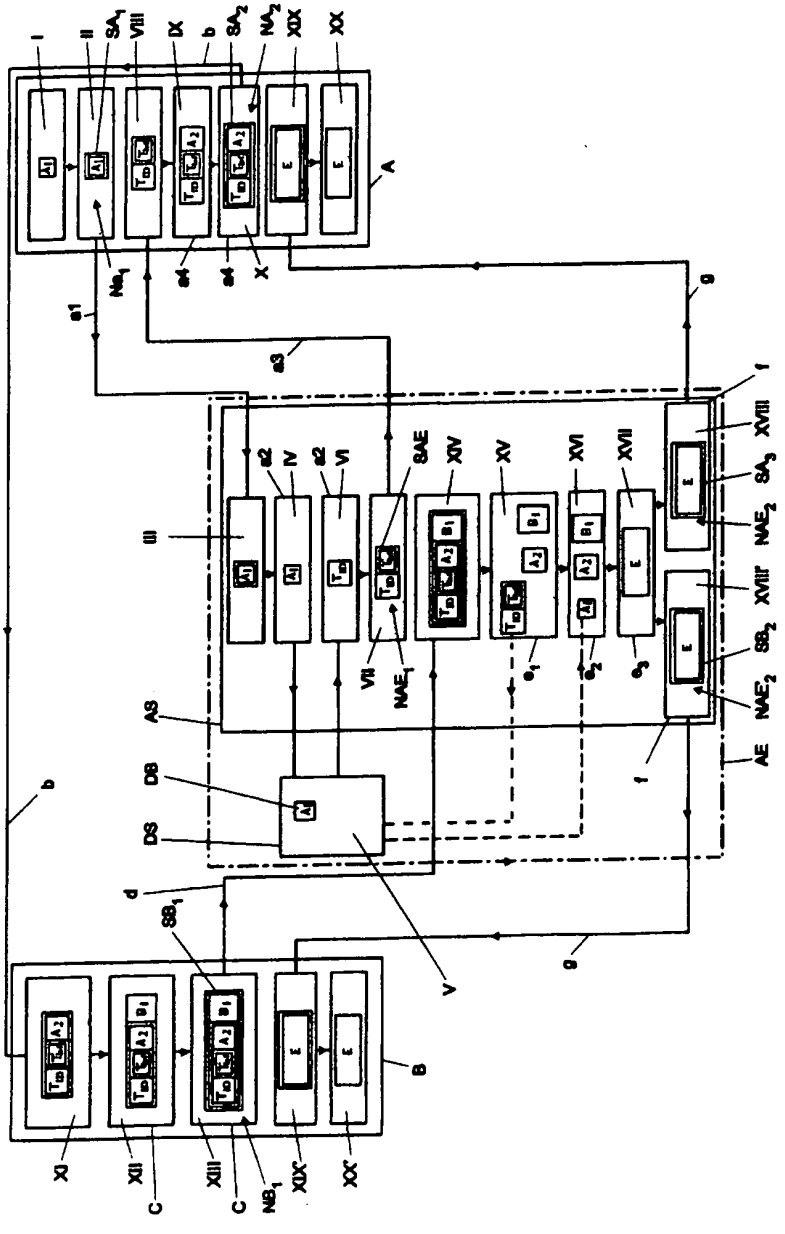


Fig. 2