(19) Deutsches Patent- und Markenamt

(10) **DE 11 2012 000 358 T5** 2013.10.17

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2012/117347**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2012 000 358.6**
(86) PCT-Aktenzeichen: **PCT/IB2012/050925**
(86) PCT-Anmeldetag: **28.02.2012**
(87) PCT-Veröffentlichungstag: **07.09.2012**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **17.10.2013**

(51) Int Cl.: ***H04L 9/00*** (2013.01)

(30) Unionspriorität:
11156518.0 **02.03.2011** **EP**

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

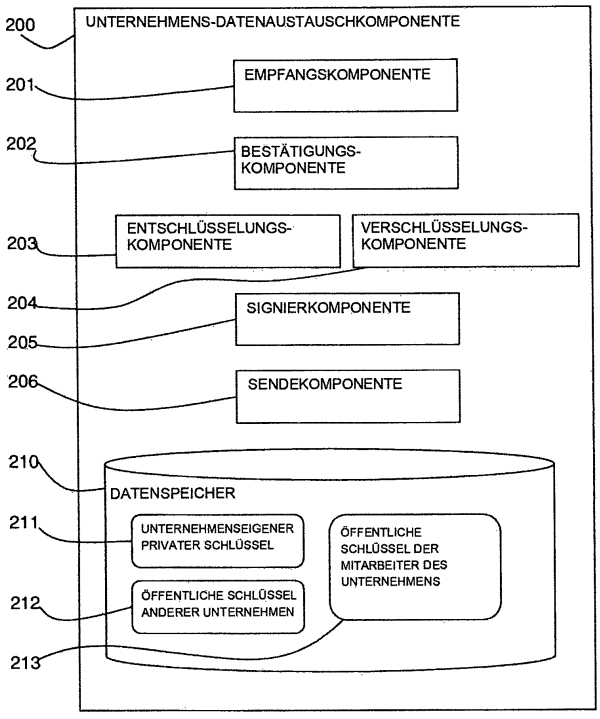
(74) Vertreter:
RICHARDT PATENTANWÄLTE GbR, 65185, Wiesbaden, DE

(72) Erfinder:
Paice, Christopher Colin, Hursley, Hampshire, GB; Chatt, Alan James, Hursley, Hampshire, GB; Stewart, Cyril, Hursley, Hampshire, GB

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Unternehmensübergreifender Datenaustausch**

(57) Zusammenfassung: Es werden ein Verfahren und ein System für den unternehmensübergreifenden Datenaustausch bereitgestellt, bei dem zwischengeschaltete Datenaustauschkomponenten einen unternehmensübergreifenden Datenaustausch durchführen. Ein Verfahren in einem ersten sendenden Unternehmen beinhaltet: Empfangen einer signierten, verschlüsselten Nachricht von einem Absender innerhalb eines ersten Unternehmens; Bestätigen des Absenders; Entschlüsseln der Nachricht; Verschlüsseln der Nachricht für den Empfang durch ein zweites Unternehmen; Signieren der verschlüsselten Nachricht durch das erste Unternehmen; und Senden der erneut signierten, erneut verschlüsselten Nachricht an ein zweites Unternehmen. Das Verfahren in einem zweiten empfangenden Unternehmen beinhaltet: Empfangen einer signierten, verschlüsselten Nachricht von einem ersten Unternehmen; Bestätigen des Absenders als das erste Unternehmen; Entschlüsseln der Nachricht; Verschlüsseln der Nachricht zum Empfang durch einen oder mehrere Empfänger im zweiten Unternehmen; Signieren der verschlüsselten Nachricht durch das zweite Unternehmen und somit Angeben, dass sie vom ersten Unternehmen stammt; und Senden der erneut signierten, erneut verschlüsselten Nachricht an den einen oder mehrere Empfänger.



Beschreibung

[0001] Diese Erfindung betrifft das Gebiet des unternehmensübergreifenden Datenaustauschs. Insbesondere betrifft die Erfindung den unternehmensübergreifenden Datenaustausch unter Verwendung digitaler Zertifikate.

[0002] Beim Senden verschlüsselter Daten unter Verwendung der dem Public Key Cryptography Standard (PKCS) entsprechenden Software werden die eindeutigen Namen (Distinguished Names DN) der Empfänger angegeben. Beim Empfangen verschlüsselter Informationen kann der DN des Absenders geprüft werden, um sicher zu gehen, dass er auf der erwarteten Absenderliste steht. Die Empfänger- und Absenderlisten in einem Unternehmen werden gepflegt, und diese Listen können lang sein und ständiges Aktualisieren erfordern, wenn Personen in ein Unternehmen eintreten oder dieses verlassen.

[0003] Es wird ein Beispiel eines Unternehmens E1 mit einer Abteilung aus drei Personen (E1S1, E1S2 und E1S3) betrachtet, die verschlüsselte Nachrichten an ein anderes Unternehmen E2 senden. Im Unternehmen E2 gibt es drei Personen (E2R1, E2R2, E2R3), die zum Empfangen und Entschlüsseln der Nachrichten berechtigt sind.

[0004] Eine Nachricht von einem Absender (E1S1, E1S2 oder E1S3) von E1 würde für die vorgesehenen Empfänger E2R1, E2R2, E2R3 im Unternehmen E2 mit dem öffentlichen Schlüssel verschlüsselt und mit dem privaten Schlüssel des Absenders signiert (E1S1, E1S2 oder E1S3). Diese wird dann an das Unternehmen E2 gesendet.

[0005] Jede der drei Personen E2R1, E2R2 und E2R3 im Unternehmen E2 kann die Nachricht entschlüsseln, weil der verschlüsselte Code für sie verschlüsselt wurde. Andere Benutzer können die Nachricht ohne Zugang zu den privaten Schlüsseln der drei Benutzer nicht entschlüsseln.

[0006] In Unternehmen E2 gibt es eine Liste berechtigter Absender, die in diesem Fall E1P1, E2P2 und E2P3 sind (es könnte auch E3S1, E4S1 etc. von anderen Unternehmen geben), deren Signatur in der empfangenen Nachricht geprüft wird.

[0007] Wenn jemand in ein Unternehmen eintritt und berechtigt ist, verschlüsselte Daten zu senden, ist es notwendig, alle möglichen Empfänger in diesem und anderen Unternehmen darüber zu informieren, dass der Liste berechtigter Absender ein neuer Name hinzugefügt werden soll.

[0008] Genauso muss, wenn jemand in ein Unternehmen eintritt und verschlüsselte Daten empfangen darf, der Name des Empfängers der Liste berechtigter Empfänger in jedem Unternehmen hinzugefügt werden, das verschlüsselte Nachrichten sendet.

[0009] Wenn jemand ausscheidet, muss sein Name aus den Listen berechtigter Absender bzw. Empfänger in allen Unternehmen entfernt werden.

[0010] Diese Arbeit der Listenpflege ist komplex und fehleranfällig. Beispielsweise ist ein Unternehmen bei der Aktualisierung der Festlegungen möglicherweise langsam, und so kommen Fehler beim Senden von Daten vor, weil Personen nicht berechtigt sind.

[0011] Deshalb besteht eine Notwendigkeit in der Technik, das oben genannte Problem anzugehen.

[0012] Gemäß einem ersten Aspekt der vorliegenden Erfindung wird ein Verfahren für den unternehmensübergreifenden Datenaustausch bei einem ersten sendenden Unternehmen bereitgestellt, das aufweist: Empfangen einer signierten, verschlüsselten Nachricht von einem Absender innerhalb eines ersten Unternehmens; Bestätigen des Absenders; Entschlüsseln der Nachricht; Verschlüsseln der Nachricht für den Empfang durch ein zweites Unternehmen; Signieren der verschlüsselten Nachricht durch das erste Unternehmen; und Senden der erneut signierten, erneut verschlüsselten Nachricht an ein zweites Unternehmen.

[0013] Gemäß einem zweiten Aspekt der vorliegenden Erfindung wird ein Verfahren für den unternehmensübergreifenden Datenaustausch bei einem zweiten empfangenden Unternehmen bereitgestellt, das aufweist: Empfangen einer signierten, verschlüsselten Nachricht von einem ersten Unternehmen; Bestätigen des Absenders als das erste Unternehmen; Entschlüsseln der Nachricht; Verschlüsseln der Nachricht zum Empfang durch einen oder mehrere Empfänger im zweiten Unternehmen; Signieren der verschlüsselten Nachricht durch das zweite Unternehmen und somit Angeben, dass sie vom ersten Unternehmen stammt; und Senden der erneut signierten, erneut verschlüsselten Nachricht an den einen oder mehrere Empfänger.

[0014] Gemäß einem dritten Aspekt der vorliegenden Erfindung wird ein System für den unternehmensübergreifenden Datenaustausch bereitgestellt, das aufweist: eine Datenaustauschkomponente, die bei einem Unternehmen als Vermittler für den Datenaustausch mit einem anderen Unternehmen bereitgestellt wird, wobei die Komponente beinhaltet: eine Empfangskomponente zum Empfangen einer verschlüsselten, signierten Nachricht; eine Bestätigungskomponente zum Bestätigen des Absenders; eine Entschlüsselungskomponente zum Entschlüsseln der Nachricht; eine Verschlüsselungskomponente zum Verschlüsseln der Nachricht zum Empfang durch einen Empfänger; eine Signierkomponen-

te zum Signieren der verschlüsselten Nachricht durch die Datenaustauschkomponente; und eine Sendekomponente zum Senden der erneut signierten, erneut verschlüsselten Nachricht an einen Empfänger.

[0015] Gemäß einem vierten Aspekt der vorliegenden Erfindung wird ein Computerprogramm bereitgestellt, das auf einem computerlesbaren Medium gespeichert und in den internen Speicher eines digitalen Computers ladbar ist und Teile von Softwarecode zum Durchführen des Verfahrens des ersten Aspekts der vorliegenden Erfindung aufweist, wenn das Programm auf einem Computer ausgeführt wird.

[0016] Gemäß einem fünften Aspekt der vorliegenden Erfindung wird ein Computerprogramm bereitgestellt, das auf einem computerlesbaren Medium gespeichert und in den internen Speicher eines digitalen Computers ladbar ist und Teile von Softwarecode zum Durchführen des Verfahrens des zweiten Aspekts der vorliegenden Erfindung aufweist, wenn das Programm auf einem Computer ausgeführt wird.

[0017] Der als die Erfindung betrachtete Gegenstand wird im Schlussteil der Spezifikation besonders herausgestellt und ausdrücklich beansprucht. Die Erfindung sowohl hinsichtlich der Organisation und des Verfahrens der Funktion, zusammen mit ihren Zielen, Merkmalen und Vorteilen, kann jedoch am besten unter Bezugnahme auf die folgende detaillierte Beschreibung verstanden werden, wenn sie in Verbindung mit den beigefügten Zeichnungen gelesen wird, wobei:

[0018] Fig. 1 ein Blockschaubild eines Systems gemäß der vorliegenden Erfindung ist;

[0019] Fig. 2 ein Blockschaubild eines Systems gemäß der vorliegenden Erfindung ist;

[0020] Fig. 3 ein Blockschaubild eines Computersystems ist, in dem die vorliegende Erfindung realisiert werden kann;

[0021] Fig. 4A ein Ablaufplan eines Verfahrens des Sendens einer Nachricht gemäß einer ersten Ausführungsform der vorliegenden Erfindung ist.

[0022] Fig. 4B ein Ablaufplan eines Verfahrens des Empfangens einer Nachricht gemäß einer ersten Ausführungsform der vorliegenden Erfindung ist;

[0023] Fig. 5A ein Ablaufplan eines Verfahrens des Sendens einer Nachricht gemäß einer zweiten Ausführungsform der vorliegenden Erfindung ist; und

[0024] Fig. 5B ein Ablaufplan eines Verfahrens des Empfangens einer Nachricht gemäß einer zweiten Ausführungsform der vorliegenden Erfindung ist;

[0025] Es ist verständlich, dass aus Gründen der Einfachheit und Übersichtlichkeit der Veranschaulichung die in den Figuren dargestellten Elemente nicht unbedingt maßstabsgerechnet gezeichnet wurden. Beispielsweise können die Abmessungen mancher der Elemente relativ zu anderen Elementen aus Gründen der Übersichtlichkeit übertrieben dargestellt sein. Ferner können Bezugszahlen in den Figuren wiederholt dargestellt sein, um entsprechende oder analoge Merkmale zu bezeichnen.

[0026] In der folgenden detaillierten Beschreibung werden zahlreiche bestimmte Einzelheiten dargelegt, um ein gründliches Verständnis der Erfindung bereitzustellen. Es ist jedoch für einen Fachmann ersichtlich, dass die vorliegende Erfindung ohne diese besonderen Einzelheiten umgesetzt werden kann. In anderen Beispielen wurden bekannte Verfahren, Vorgehensweisen und Komponenten nicht im Einzelnen beschrieben, um die vorliegende Erfindung nicht zu verunklaren.

[0027] An den Rändern des Unternehmens, wo Daten an ein anderes Unternehmen gesendet werden, wird eine Komponente bereitgestellt, die durch Entschlüsseln und erneutes Verschlüsseln der Daten den Namen des einzelnen Absenders entfernt und ihn durch einen Unternehmensnamen ersetzt.

[0028] Der Ausdruck Unternehmen wird für jede Organisation mit mehreren Absendern und Empfängern verwendet. Die Absender und Empfänger können Einzelpersonen oder Gruppen innerhalb eines Unternehmens sein. Die Absender und Empfänger können jeweils einen eindeutigen Namen haben.

[0029] Im beschriebenen System kann eine Liste berechtigter Absender bei einem Unternehmen nur einen eindeutigen Unternehmensnamen aufweisen. Genauso kann im Unternehmen am Empfangsende eine Liste berechtigter Empfänger erstellt werden. Dies erfolgt im Bereich des Unternehmens und ist daher sehr einfach zu verwalten.

[0030] Sobald die Unternehmensnamen erstellt sind, ist es nicht notwendig, andere Unternehmen zu informieren, wenn die internen Nutzer in einem Unternehmen wechseln.

[0031] Auf Fig. 1 Bezug nehmend, zeigt ein Blockschaubild **100** den Datenaustausch zwischen zwei Unternehmen. Ein erstes Unternehmen **110** hat mehrere Absender **111** bis **114**, die eine verschlüsselte Nachricht an die Empfänger **121** bis **124** in einem zweiten Unternehmen **120** senden möchten.

[0032] Im beschriebenen System wird eine erste Unternehmens-Datenaustauschkomponente **115** im ersten Unternehmen **110** bereitgestellt, die den Datenaustausch mit anderen Unternehmen wie bei-

spielsweise dem zweiten Unternehmen **120** abwickelt. Die erste Unternehmens-Datenaustauschkomponente **115** beinhaltet den Datenspeicher mit einer Liste **116** berechtigter Absender **111** bis **114** aus dem ersten Unternehmen **110**. Der Datenspeicher kann auch eine Liste **117** anderer Unternehmen enthalten (z. B. das zweite Unternehmen **120**), mit denen das erste Unternehmen **110** Daten austauscht.

[0033] Im zweiten Unternehmen **120** wird eine zweite Unternehmens-Datenaustauschkomponente **125** bereitgestellt, die den Datenaustausch mit anderen Unternehmen wie beispielsweise dem ersten Unternehmen **110** abwickelt. Die zweite Unternehmens-Datenaustauschkomponente **125** beinhaltet den Datenspeicher mit einer Liste **126** berechtigter Absender **121** bis **124** aus dem zweiten Unternehmen **120**. Der Datenspeicher kann auch eine Liste **127** anderer Unternehmen enthalten (z. B. das erste Unternehmen **110**), mit denen das zweite Unternehmen **120** Daten austauscht.

[0034] Jedes von dem ersten und zweiten Unternehmen **110** und **120** kann Absender und Empfänger beinhalten und die erste und die zweite Unternehmens-Datenaustauschkomponente **115** und **125** können die beiden Listen **116** und **126** berechtigter Absender und Empfänger aus ihrem Unternehmen **110** bzw. **120** beinhalten. Ein Unternehmen kann mit vielen anderen Unternehmen Daten austauschen.

[0035] Auf Fig. 2 Bezug nehmend, zeigt ein Blockschaubild eine Unternehmens-Datenaustauschkomponente **200**, die in einem Unternehmen als eine Einheit oder Anwendung bereitgestellt werden kann, um als Vermittler zwischen den Absendern und Empfängern verschiedener Unternehmen zu fungieren.

[0036] Die Unternehmens-Datenaustauschkomponente **200** beinhaltet die folgenden Komponenten, die sowohl einer Empfangs- als auch einer Sendefunktion der Unternehmens-Datenaustauschkomponente **200** gemeinsam sind.

[0037] Zum Empfangen einer verschlüsselten und signierten Nachricht wird eine Empfangskomponente **201** bereitgestellt. Diese Nachricht kann im Fall einer gesendeten Nachricht von innerhalb des Unternehmens empfangen oder im Fall einer empfangenen Nachricht von einem anderen Unternehmen empfangen werden.

[0038] Zum Prüfen einer digitalen Signatur in der empfangenen Nachricht wird eine Bestätigungskomponente **202** bereitgestellt.

[0039] Eine Entschlüsselungskomponente **203** und eine Verschlüsselungskomponente **204** werden zum Entschlüsseln und erneuten Verschlüsseln der Nachricht bereitgestellt. Die Entschlüsselung und erneute Verschlüsselung kann in umgekehrter Reihenfolge erfolgen (erneute Verschlüsselung vor Entschlüsselung), um die Dateien in verschlüsselter Form und nicht im Klartext zu erhalten

[0040] Zum Signieren der erneut verschlüsselten Nachricht wird eine Signierkomponente **205** bereitgestellt.

[0041] Zum Senden der erneut verschlüsselten Nachricht wird eine Sendekomponente **206** bereitgestellt. Diese Nachricht kann im Fall einer gesendeten Nachricht an ein anderes Unternehmen gesendet oder in Fall einer empfangenen Nachricht an Empfänger innerhalb des Unternehmens gesendet werden.

[0042] Zwei oder mehr der oben genannten Komponenten können miteinander kombiniert werden, beispielsweise dort, wo ein kombiniertes Signier- und Verschlüsselungszertifikat verwendet wird.

[0043] Die Unternehmens-Datenaustauschkomponente **200** beinhaltet oder hat Zugriff auf den Datenspeicher **210**, der den unternehmenseigenen privaten Schlüssel **211**, eine Liste **212** der öffentlichen Schlüssel anderer Unternehmen und eine Liste **213** der öffentlichen Schlüssel der unternehmenseigenen Mitarbeiter speichert.

[0044] Die Public-Key-Kryptographie (Kryptographie mit öffentlichem Schlüssel) ist ein kryptographischer Ansatz, der die Verwendung asymmetrischer Schlüsselalgorithmen beinhaltet. Die asymmetrischen Schlüsselalgorithmen dienen dazu, ein mathematisch miteinander in Beziehung stehendes Schlüsselpaar zu erzeugen: einen geheimen privaten Schlüssel und einen veröffentlichten öffentlichen Schlüssel. Die Verwendung dieser Schlüssel ermöglicht den Schutz der Echtheit einer Nachricht durch Erzeugen einer digitalen Signatur einer Nachricht mit dem privaten Schlüssel, die mit dem öffentlichen Schlüssel überprüft werden kann. Sie ermöglicht außerdem den Schutz der Vertraulichkeit und Integrität einer Nachricht durch Public-Key-Verschlüsselung, wobei die Nachricht mit dem öffentlichen Schlüssel verschlüsselt wird und nur mit dem privaten Schlüssel entschlüsselt werden kann.

[0045] Auf Fig. 3 Bezug nehmend, beinhaltet ein beispielhaftes System zum Realisieren von Aspekten der Erfindung ein zum Speichern und/oder Ausführen von Programmcode geeignetes Datenverarbeitungssystem **300** mit mindestens einem Prozessor **301**, der über ein Bussystem **303** direkt oder indirekt mit Speicherelementen gekoppelt ist. Die Speicherelemente können unter anderem ein lokaler Speicher, der während der eigentlichen Ausführung des Programmcodes verwendet wird, ein Massenspeicher und Zwischenspeicher sein, die eine vorübergehende Speicherung von mindestens etwas Programm-

code bereitstellen, um die Anzahl der Male zu verringern, die der Programmcode während der Ausführung aus dem Massenspeicher abgerufen werden muss.

[0046] Die Speicherelemente können Systemspeicher **302** in Form eines Nur-Lese-Speichers (ROM) **304** und eines Schreib-Lese-Speichers (RAM) **305** sein. Im ROM **304** kann ein Basic Input/Output System (BIOS) **306** gespeichert sein. Die System-Software **307** einschließlich der Betriebssystem-Software **308** kann im RAM **305** gespeichert sein. Im RAM **305** können auch Software-Anwendungen **310** gespeichert sein.

[0047] Das System **300** kann auch ein primäres Speichermittel **311** wie ein magnetisches Festplattenlaufwerk und sekundäre Speichermittel **312** wie ein Laufwerk für eine magnetische und ein Laufwerk für eine optische Speicherplatte enthalten. Die Laufwerke und ihre zugehörigen computerlesbaren Medien bieten eine nicht-flüchtige Speicherung von computerausführbaren Anweisungen, Datenstrukturen, Programmmodulen und anderen Daten für das System **300**. Die Software-Anwendungen können auf dem primären und dem sekundären Speichermittel **311** und **312** sowie im Systemspeicher **302** gespeichert sein.

[0048] Über einen Netzwerkadapter **316** kann das Datenverarbeitungssystem **300** in einer vernetzten Umgebung mit logischen Verbindungen zu einem oder mehreren entfernt angeordneten Computern betrieben werden.

[0049] Eingangs-/Ausgangseinheiten **313** können entweder direkt oder durch zwischengeschaltete E/A-Steuereinheiten an das System gekoppelt sein. Über Eingabeeinheiten wie eine Tastatur, eine Zeigeeinheit oder andere Eingabeeinheiten (z. B. Mikrophon, Joystick, Gamepad, Satellitenschüssel, Scanner oder Ähnliches) kann ein Benutzer Befehle und Daten in das System **300** eingeben. Ausgabeeinheiten können unter anderem Lautsprecher, Drucker etc. sein. Eine Anzeigeeinheit **314** ist ebenfalls über eine Schnittstelle wie beispielsweise den Video-Adapter **315** mit dem Systembus **303** verbunden.

[0050] Auf die Fig. 4A und Fig. 4B Bezug nehmend, zeigen die schematischen Ablaufpläne **400** und **450** eine erste Ausführungsform eines Verfahrens des Sendens einer unternehmensübergreifenden Nachricht bzw. eines Verfahrens des Empfangens einer unternehmensübergreifenden Nachricht.

[0051] Fig. 4A zeigt einen Ablaufplan **400** eines Verfahrens des Sendens einer unternehmensübergreifenden Nachricht durch eine Unternehmens-Datenaustauschkomponente, die im sendenden Unternehmen E1 bereitgestellt wird.

[0052] Die Unternehmens-Datenaustauschkomponente empfängt **401** in E1 eine verschlüsselte, signierte Nachricht von S1, wobei S1 ein Absender innerhalb des Unternehmens E1 ist. Die verschlüsselte Nachricht **411** ist mit dem öffentlichen Schlüssel von E1 **412** verschlüsselt und mit dem privaten Schlüssel von S1 **414** signiert **413**.

[0053] Die Komponente bestätigt **402** die Nachricht mit ihrem gespeicherten öffentlichen Schlüssel von S1 aus ihrer Liste berechtigter Absender innerhalb ihres Unternehmens. Das Ergebnis ist die verschlüsselte Nachricht **411**, die mit dem öffentlichen Schlüssel von E1 **412** verschlüsselt wurde.

[0054] Die Komponente entschlüsselt **403** die verschlüsselte Nachricht mit ihrem eigenen privaten Schlüssel E1, so dass sich eine Klartext-Nachricht **415** ergibt.

[0055] Die Komponente verschlüsselt **404** dann die Nachricht mit dem öffentlichen Schlüssel E2 des Unternehmens E2, an das die Nachricht gesendet werden soll, aus der gespeicherten Liste der öffentlichen Schlüssel von Unternehmen, mit denen die Komponente Daten austauschen darf. Das Ergebnis ist die verschlüsselte Nachricht **416**, die mit dem öffentlichen Schlüssel E2 **417** verschlüsselt wurde.

[0056] Die Komponente signiert **405** dann die Nachricht mit dem privaten Schlüssel des Unternehmens E1. Das Ergebnis ist eine verschlüsselte Nachricht **416**, die mit dem öffentlichen Schlüssel von E2 **417** verschlüsselt und mit dem privaten Schlüssel von E1 **419** signiert **418** wurde.

[0057] Die verschlüsselte, signierte Nachricht **418** wird vom Unternehmen E1 an das Unternehmen E2 gesendet **406**.

[0058] Fig. 4B zeigt einen Ablaufplan **450** eines Verfahrens des Empfangens einer unternehmensübergreifenden Nachricht durch eine Unternehmens-Datenaustauschkomponente, die im empfangenden Unternehmen E2 bereitgestellt wird.

[0059] Die Unternehmens-Datenaustauschkomponente empfängt **451** in E2 eine verschlüsselte, signierte Nachricht von einem anderen Unternehmen E1. Die verschlüsselte Nachricht **461** ist mit dem öffentlichen Schlüssel von E2 **462** verschlüsselt und mit dem privaten Schlüssel von E1 **464** signiert **463**.

[0060] Die Komponente bestätigt **452** die Nachricht mit ihrem gespeicherten öffentlichen Schlüssel E1 aus ihrer Liste berechtigter Unternehmen, von denen sie Nachrichten empfangen darf. Das Ergebnis ist die verschlüsselte Nachricht **461**, die mit dem öffentlichen Schlüssel von E2 **462** verschlüsselt wurde.

[0061] Die Komponente entschlüsselt **453** die verschlüsselte Nachricht mit ihrem eigenen privaten Schlüssel E2, so dass sich eine Klartext-Nachricht **465** ergibt.

[0062] Die Komponente verschlüsselt **454** dann mit dem öffentlichen Schlüssel von R1 bis Rm die Nachricht einzeln für die Empfänger R1 bis Rm. Die öffentlichen Schlüssel von R1 bis Rm werden auf einer gespeicherten Liste berechtigter Empfänger innerhalb des Unternehmens E2 bereitgestellt, bei dem die Komponente in Betrieb ist. Das Ergebnis ist eine Vielzahl verschlüsselter Nachrichten **466A** bis C, von denen jede mit einem der öffentlichen Schlüssel R1 bis Rm **467A** verschlüsselt wurde.

[0063] Die Komponente signiert **455** dann die verschlüsselten Nachrichten mit dem privaten Schlüssel des Unternehmens E2. Die Ergebnisse sind verschlüsselte Nachrichten **466A** bis C, von denen jede mit den öffentlichen Schlüsseln von R1 bis Rm **467A** verschlüsselt und mit dem privaten Schlüssel von E2 **469** signiert **468A** bis C wurde.

[0064] Die verschlüsselten Nachrichten **468A** bis C werden von der Komponente im Unternehmen E2 an ihre berechtigten Empfänger innerhalb des Unternehmens E2 gesendet **456**.

[0065] Auf die Fig. 5A und Fig. 5B Bezug nehmend, zeigen die schematischen Ablaufpläne **500** und **550** eine zweite Ausführungsform eines Verfahrens des Sendens einer unternehmensübergreifenden Nachricht bzw. eines Verfahrens des Empfangens einer unternehmensübergreifenden Nachricht. Bei der zweiten Ausführungsform werden die Nachrichten vor dem Entschlüsseln erneut verschlüsselt, um ein Offenbaren der Klartext-Nachricht zu vermeiden.

[0066] Fig. 5A zeigt einen Ablaufplan **500** eines Verfahrens des Sendens einer unternehmensübergreifenden Nachricht durch eine Unternehmens-Datenaustauschkomponente, die beim sendenden Unternehmen E1 bereitgestellt wird.

[0067] Die Unternehmens-Datenaustauschkomponente empfängt **501** in E1 eine verschlüsselte, signierte Nachricht von S1, wobei S1 ein Absender innerhalb des Unternehmens E1 ist. Die verschlüsselte Nachricht **511** ist mit dem öffentlichen Schlüssel von E1 **512** verschlüsselt und mit dem privaten Schlüssel von S1 **514** signiert **513**.

[0068] Die Komponente bestätigt **502** die Nachricht mit dem gespeicherten öffentlichen Schlüssel S1 aus ihrer Liste berechtigter Absender innerhalb ihres Unternehmens. Das Ergebnis ist die verschlüsselte Nachricht **511**, die mit dem öffentlichen Schlüssel von E1 **512** verschlüsselt wurde.

[0069] Die Komponente verschlüsselt **503** dann die Nachricht mit dem öffentlichen Schlüssel E2 des Unternehmens E2, an das die Nachricht gesendet werden soll, aus der gespeicherten Liste der öffentlichen Schlüssel von Unternehmen, mit denen die Komponente Daten austauschen darf. Das Ergebnis ist die verschlüsselte Nachricht **516**, die mit dem öffentlichen Schlüssel E2 **517** der verschlüsselten Nachricht **511** verschlüsselt wurde, die mit dem öffentlichen Schlüssel E1 **512** verschlüsselt wurde.

[0070] Die Komponente entschlüsselt **504** die verschlüsselte Nachricht **511** mit ihrem eigenen privaten Schlüssel E1, so dass sich eine verschlüsselte Nachricht **516** ergibt, die mit dem öffentlichen Schlüssel E2 **517** verschlüsselt wurde. Auf diese Weise wird der Klartext nicht offenbart.

[0071] Die Komponente signiert **505** dann die Nachricht mit dem privaten Schlüssel des Unternehmens E1. Das Ergebnis ist eine verschlüsselte Nachricht **516**, die mit dem öffentlichen Schlüssel von E2 **517** verschlüsselt und mit dem privaten Schlüssel von E1 **519** signiert **518** wurde.

[0072] Die verschlüsselte signierte Nachricht wird vom Unternehmen E1 an das Unternehmen E2 gesendet **506**.

[0073] Fig. 5B zeigt einen Ablaufplan **550** eines Verfahrens des Empfangens einer unternehmensübergreifenden Nachricht durch eine Unternehmens-Datenaustauschkomponente, die im empfangenden Unternehmen E2 bereitgestellt wird.

[0074] Die Unternehmens-Datenaustauschkomponente empfängt **551** in E2 eine verschlüsselte, signierte Nachricht von einem anderen Unternehmen E1. Die verschlüsselte Nachricht **561** ist mit dem öffentlichen Schlüssel von E2 **562** verschlüsselt und mit dem privaten Schlüssel von E1 **564** signiert **563**.

[0075] Die Komponente bestätigt **552** die Nachricht mit ihrem gespeicherten öffentlichen Schlüssel E1 aus ihrer Liste berechtigter Unternehmen, von denen sie Nachrichten empfangen darf. Das Ergebnis ist die verschlüsselte Nachricht **561**, die mit dem öffentlichen Schlüssel von E2 **562** verschlüsselt wurde.

[0076] Die Komponente verschlüsselt **553** dann mit dem öffentlichen Schlüssel von R1 bis Rm die Nachricht einzeln für die Empfänger R1 bis Rm im Unternehmen E2. Die öffentlichen Schlüssel von R1 bis Rm werden auf einer gespeicherten Liste berechtigter Empfänger innerhalb des Unternehmens E2 bereitgestellt, bei dem die Komponente in Betrieb ist. Das Ergebnis ist eine Vielzahl verschlüsselter Nachrichten **566A** bis C, von denen jede mit einem der öffentlichen Schlüssel R1 bis Rm **567A** der verschlüsselten Nachricht **561** verschlüsselt wurde, die mit

dem öffentlichen Schlüssel E2 **562** verschlüsselt wurde.

[0077] Die Komponente entschlüsselt **554** die verschlüsselte Nachricht **561** mit ihrem eigenen privaten Schlüssel E2, so dass sich verschlüsselte Nachrichten **566A** bis C ergeben, die mit einem der öffentlichen Schlüssel R1 bis Rm **567A** verschlüsselt wurden. Auf diese Weise wird der Klartext nicht offenbart.

[0078] Die Komponente signiert **555** dann die verschlüsselten Nachrichten mit dem privaten Schlüssel des Unternehmens E2. Die Ergebnisse sind verschlüsselte Nachrichten **566A** bis C, von denen jede mit den öffentlichen Schlüsseln von R1 bis Rm **567A** verschlüsselt und mit dem privaten Schlüssel von E2 **569** signiert **568A** bis C wurde.

[0079] Die verschlüsselten, signierten Nachrichten **566A** bis C werden von der Komponente im Unternehmen E2 an ihre berechtigten Empfänger innerhalb des Unternehmens E2 gesendet **556**.

[0080] Das beschriebene System hat logisch zwei Teile, die in einem Absender- und einem Empfängerunternehmen jeweils spiegelbildlich zueinander funktionieren. Sie können unabhängig voneinander realisiert werden und bestehen. Die Funktionalität kann auch in einer einzigen Komponente kombiniert werden.

[0081] Im beschriebenen System gibt es im Unternehmen E1 nur einen Empfänger, der für das andere Unternehmen gekennzeichnet wird, beispielsweise mit einem eindeutigen Namen E1E2. Die Nachricht wird nur für den Datenaustausch zwischen dem Unternehmen E1 und dem Unternehmen E2 verschlüsselt und signiert. Ebenso wie dadurch die Verwaltung der eindeutigen Namen vereinfacht wird, muss in der Maschine der Sendekomponente weniger Arbeit geleistet werden, so dass CPU eingespart wird.

[0082] Logisch besteht zwischen den beiden Unternehmen eine Verbindung (z. B. ein Stück Leitung). An einem Ende der Leitung im Unternehmen E1 gibt es eine Komponente beispielsweise in der Form einer Anwendung oder Vorrichtung, die das private Zertifikat für E1E2 hat. Diese Komponente leistet Folgendes:

- bestätigt die Daten;
- entschlüsselt den Schlüssel, der zum Verschlüsseln der Daten verwendet wurde;
- verschlüsselt die Daten erneut mit dem öffentlichen Zertifikat „Unternehmen E2" für das andere Unternehmen;
- signiert mit dem Zertifikat „Unternehmen E1"; und
- sendet diese Daten.

[0083] Am Ende der Leitung auf der Seite des Unternehmens E2 gibt es eine Komponente, die Folgendes leistet:

- bestätigt, dass die Daten gültig sind, indem sie das Zertifikat mit dem öffentlichen Zertifikat „Unternehmen E1" prüft;
- die Nachricht mit dem privaten Schlüssel „Unternehmen E2" entschlüsselt;
- eine Liste der möglichen Empfänger pflegt – dies variiert typischerweise mit der Anwendung. Jeder mögliche Empfänger hat ein öffentliches Zertifikat;
- verschlüsselt die Daten mit ihrem öffentlichen Schlüssel erneut für jeden Empfänger;
- signiert mit einem Schlüssel, genannt „von_ E1" (vollständig im Besitz von E2, wobei der Name angibt, von wem die Nachricht stammt);
- sendet die Daten an ihre Ziele weiter.

[0084] Berechtigte Empfänger empfangen die Nachricht, die mit „von_E1" signiert wurde, so dass erkannt werden kann, dass sie ursprünglich vom Unternehmen E1 stammt.

[0085] Wenn eine Person oder neue Gruppe in das Unternehmen E1 eintritt, wird die Liste der Absender in der Komponente am Ende der Leitung auf der Seite des sendenden Unternehmens E1 aktualisiert. Dies erfolgt vollständig unter der Kontrolle des Unternehmens E1.

[0086] Wenn jemand oder eine Gruppe als ein neuer Empfänger in das Unternehmen E2 eintritt, muss das Unternehmen E1 nicht darüber informiert werden. Nur die Komponente am Ende der Leitung auf der Seite des Unternehmens E2 muss mit den neuen Empfängern aktualisiert werden.

[0087] Es gibt zwei Ausführungsformen des beschriebenen Verfahrens und Systems. In einer ersten Ausführungsform werden keine Daten weitergeleitet, die einen ursprünglichen Absender S1 im empfangenden Unternehmen E2 kennzeichnen können. Alles was die Endempfänger R1 bis Rm in E2 sehen können, ist die Angabe E2E1. Die empfangene Nachricht bei R1 bis Rm kennzeichnet das sendende Unternehmen E1 mit einem Namen im Zertifikat. Dies könnte also „von KUNDE1" lauten oder es könnte auf den sinnvolleren Namen „von IBM" lauten (IBM ist eine Marke der International Business Machines Corporation). Dies kann vom Administrator, der das Zertifikat festlegt, definiert werden.

[0088] Diese erste Ausführungsform kann einen zuverlässigen und sicheren Mechanismus für einen „blinden" Datenaustausch bereitstellen, ohne dass der Absender die Identität des Empfängers oder der Empfänger die Identität des Absenders kennen muss. Dabei wäre es erforderlich, den Datenaustausch in beiden Richtungen zu verwalten (vom Absender zum Empfänger und wieder zurück), würde es

aber dem Empfänger oder Absender gestatten, ihre Identität von der „Außenwelt" abzuschirmen.

[0089] Bei einer zweiten Ausführungsform dürfen Daten über den ursprünglichen Absender durch den gesamten Prozess bis zu den Endempfängern R1 bis Rm weitergeleitet werden. Die ursprünglichen Daten werden vom Absender S1 signiert. Das öffentliche Zertifikat für den Absender S1 wird mit den Daten vom Unternehmen E1 und vom Unternehmen E2 an die Endempfänger R1 bis Rm weitergeleitet. Dies ermöglicht es den Endempfängern R1 bis Rm, den Urheber der Daten und die Kette der Signierer zu sehen.

[0090] Als weiteren Aspekt kann ein erstes Unternehmen E1 versuchen, eine Nachricht von einem Absender S1 zu entschlüsseln. Dabei muss E1 die Signatur des Absenders S1 haben und somit den Absender kennen. Wenn das Unternehmen E1 die Signatur bestätigen kann, kann es die Signatur weiterleiten. Wenn das Unternehmen E1 eine Liste berechtigter Absender hat, kann es sie daraufhin überprüfen, ob der Absender S1 auf der Liste steht, und wenn er nicht auf der Liste steht, wird die Nachricht nicht weitergeleitet. Dieser Aspekt kann eine Kontrolle darüber verschaffen, wer Daten an ein anderes Unternehmen sendet.

[0091] Eine Unternehmens-Datenaustauschkomponente für den unternehmensübergreifenden Datenaustausch kann einem Kundenunternehmen über ein Netzwerk als Dienstleistung bereitgestellt werden.

[0092] Die Erfindung kann die Form einer lediglich aus Hardware bestehenden Ausführungsform, einer lediglich aus Software bestehenden Ausführungsform oder einer Software- und Hardware-Elemente kombinierenden Ausführungsform annehmen. Bei einer bevorzugten Ausführungsform wird die Erfindung in Software realisiert, darunter Firmware, residente Software, Mikrocode etc., ohne darauf beschränkt zu sein.

[0093] Die Erfindung kann die Form eines Computerprogrammprodukts annehmen, das von einem computernutzbaren oder computerlesbaren Medium aus zugänglich ist, das den Programmcode zur Verwendung durch oder in Verbindung mit einem Computer oder einem beliebigen Anweisungsausführungssystem bereitstellt. Zum Zweck dieser Beschreibung kann ein computernutzbares oder computerlesbares Speichermedium jede Vorrichtung sein, die ein Programm zur Verwendung durch oder in Verbindung mit einem/r Anweisungsausführungssystem, -vorrichtung oder -einheit enthalten, speichern, übertragen, verbreiten oder transportieren kann.

[0094] Das Medium kann ein elektronisches, magnetisches, optisches, elektromagnetisches, Infrarot- oder Halbleiter-System (bzw. -Vorrichtung oder -Einheit) oder ein Verbreitungsmedium sein. Beispiele für ein computerlesbares Medium sind unter anderem ein Halbleiter- bzw. Festkörperspeicher, ein Magnetband, eine auswechselbare Computer-Diskette, ein Schreib-Lese-Speicher (RAM), ein Nur-Lese-Speicher (ROM), eine starre Magnetspeicherplatte und eine optische Speicherplatte. Aktuelle Beispiele für optische Speicherplatten sind unter anderem Compact-Disk-Nur-Lese-Speicher (CD-ROM), Compact-Disk-Schreib-Lese-Speicher (CD-R/W) und DVDs.

[0095] Verbesserungen und Modifikationen können am Vorgenannten vorgenommen werden, ohne vom Umfang der vorliegenden Erfindung abzuweichen.

Patentansprüche

1. Verfahren für den unternehmensübergreifenden Datenaustausch in einem ersten sendenden Unternehmen (**110**), das aufweist:
Empfangen (**401**, **501**) einer signierten, verschlüsselten Nachricht von einem Absender (**111** bis **114**) in einem ersten Unternehmen (**110**);
Bestätigen (**402**, **502**) des Absenders;
Entschlüsseln (**403**, **504**) der Nachricht;
Verschlüsseln (**404**, **503**) der Nachricht für den Empfang durch ein zweites Unternehmen;
Signieren (**405**, **505**) der verschlüsselten Nachricht durch das erste Unternehmen; und
Senden (**406**, **506**) der erneut signierten, erneut verschlüsselten Nachricht an ein zweites Unternehmen (**120**).

2. Verfahren nach Anspruch 1, wobei der Schritt des Verschlüsselns (**503**) durchgeführt wird, bevor die Nachricht entschlüsselt wird (**504**), um zu verhindern, dass der Klartext der Nachricht offenbart wird.

3. Verfahren nach Anspruch 1 oder 2, das beinhaltet:
Pflegen einer Liste berechtigter Absender (**116**) im ersten Unternehmen (**110**).

4. Verfahren nach einem der Ansprüche 1 bis 3, das beinhaltet:
Pflegen einer Liste zweiter Unternehmen (**117**), mit denen das erste Unternehmen (**110**) Daten austauscht.

5. Verfahren nach Anspruch 3 oder 4, wobei die Liste (**116**, **117**) eindeutige Namen kennzeichnet.

6. Verfahren nach einem der vorherigen Ansprüche, wobei Daten über den Absender vom ersten Unternehmen (**110**) zum zweiten Unternehmen (**120**) weitergeleitet werden.

7. Verfahren nach einem der vorherigen Ansprüche, wobei zum Bestätigen, Entschlüsseln, Ver-

schlüsseln und Signieren der Nachricht eine Public-Key-Kryptographie verwendet wird.

8. Verfahren für den unternehmensübergreifenden Datenaustausch in einem zweiten empfangenden Unternehmen (**120**), das aufweist:
Empfangen (**451**, **551**) einer signierten, verschlüsselten Nachricht von einem ersten Unternehmen (**110**);
Bestätigen (**452**, **552**) des Absenders als das erste Unternehmen (**110**);
Entschlüsseln (**453**, **554**) der Nachricht;
Verschlüsseln (**454**, **553**) der Nachricht zum Empfang durch einen oder mehrere Empfänger im zweiten Unternehmen (**120**);
Signieren (**455**, **555**) der verschlüsselten Nachricht durch das zweite Unternehmen (**120**) und somit Angeben, dass sie vom ersten Unternehmen (**110**) stammt; und
Senden (**456**, **556**) der erneut signierten, erneut verschlüsselten Nachricht an den einen oder mehrere Empfänger (**121** bis **124**).

9. Verfahren nach Anspruch 8, wobei der Schritt des Verschlüsselns (**553**) durchgeführt wird, bevor die Nachricht entschlüsselt wird (**554**), um zu verhindern, dass der Klartext der Nachricht offenbart wird.

10. Verfahren nach Anspruch 8 oder 9, das beinhaltet:
Pflegen einer Liste (**126**) berechtigter Empfänger im zweiten Unternehmen.

11. Verfahren nach einem der Ansprüche 8 bis 10, das beinhaltet:
Pflegen einer Liste erster Unternehmen (**127**), mit denen das zweite Unternehmen Daten austauscht.

12. Verfahren nach Anspruch 10 oder 11, wobei die Liste (**126**, **127**) eindeutige Namen kennzeichnet.

13. Verfahren nach einem der Ansprüche 8 bis 12, darunter Empfangen von Daten über einen ursprünglichen Absender der Nachricht im zweiten Unternehmen und Weiterleiten der Daten an den einen oder mehrere Empfänger.

14. Verfahren nach einem der Ansprüche 8 bis 13, wobei eine Public-Key-Kryptographie zum Bestätigen, Entschlüsseln, Verschlüsseln und Signieren der Nachricht verwendet wird.

15. System für den unternehmensübergreifenden Datenaustausch, das aufweist:
eine Datenaustauschkomponente (**200**), die in einem Unternehmen als Vermittler für den Datenaustausch mit einem anderen Unternehmen bereitgestellt wird, wobei die Komponente (**200**) beinhaltet:
eine Empfangskomponente (**201**) zum Empfangen einer verschlüsselten, signierten Nachricht;
eine Bestätigungskomponente (**202**) zum Bestätigen des Absenders;
eine Entschlüsselungskomponente (**203**) zum Entschlüsseln der Nachricht;
eine Verschlüsselungskomponente (**204**) zum Verschlüsseln der Nachricht zum Empfang durch einen Empfänger;
eine Signierkomponente (**205**) zum Signieren der verschlüsselten Nachricht durch die Datenaustauschkomponente; und
eine Sendekomponente (**206**) zum Senden der erneut signierten, erneut verschlüsselten Nachricht an einen Empfänger.

16. System nach Anspruch 15, wobei die Datenaustauschkomponente (**200**) eine Public-Key-Kryptographie verwendet.

17. System nach Anspruch 15 oder 16, wobei die Datenaustauschkomponente (**200**) in einem ersten Unternehmen (**110**) beinhaltet:
einen Datenspeicher (**210**) mit einer Liste berechtigter Absender (**116**, **213**) im ersten Unternehmen und einer Liste von Unternehmen (**117**, **212**), mit denen das erste Unternehmen Daten austauscht.

18. System nach einem der Ansprüche 15 bis 17, wobei die Datenaustauschkomponente (**200**) in einem zweiten Unternehmen (**120**) beinhaltet:
einen Datenspeicher (**210**) mit einer Liste berechtigter Empfänger (**126**, **213**) im zweiten Unternehmen und einer Liste von Unternehmen (**127**, **212**), mit denen das zweite Unternehmen Daten austauscht.

19. Computerprogramm, das auf einem computerlesbaren Medium gespeichert und in den internen Speicher eines digitalen Computers ladbar ist, das Softwareprogrammteile zum Durchführen des Verfahrens nach einem der Ansprüche 1 bis 7 aufweist, wenn das Programm auf einem Computer ausgeführt wird.

20. Computerprogramm, das auf einem computerlesbaren Medium gespeichert und in den internen Speicher eines digitalen Computers ladbar ist, das Softwareprogrammteile zum Durchführen des Verfahrens nach einem der Ansprüche 8 bis 14 aufweist, wenn das Programm auf einem Computer ausgeführt wird.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

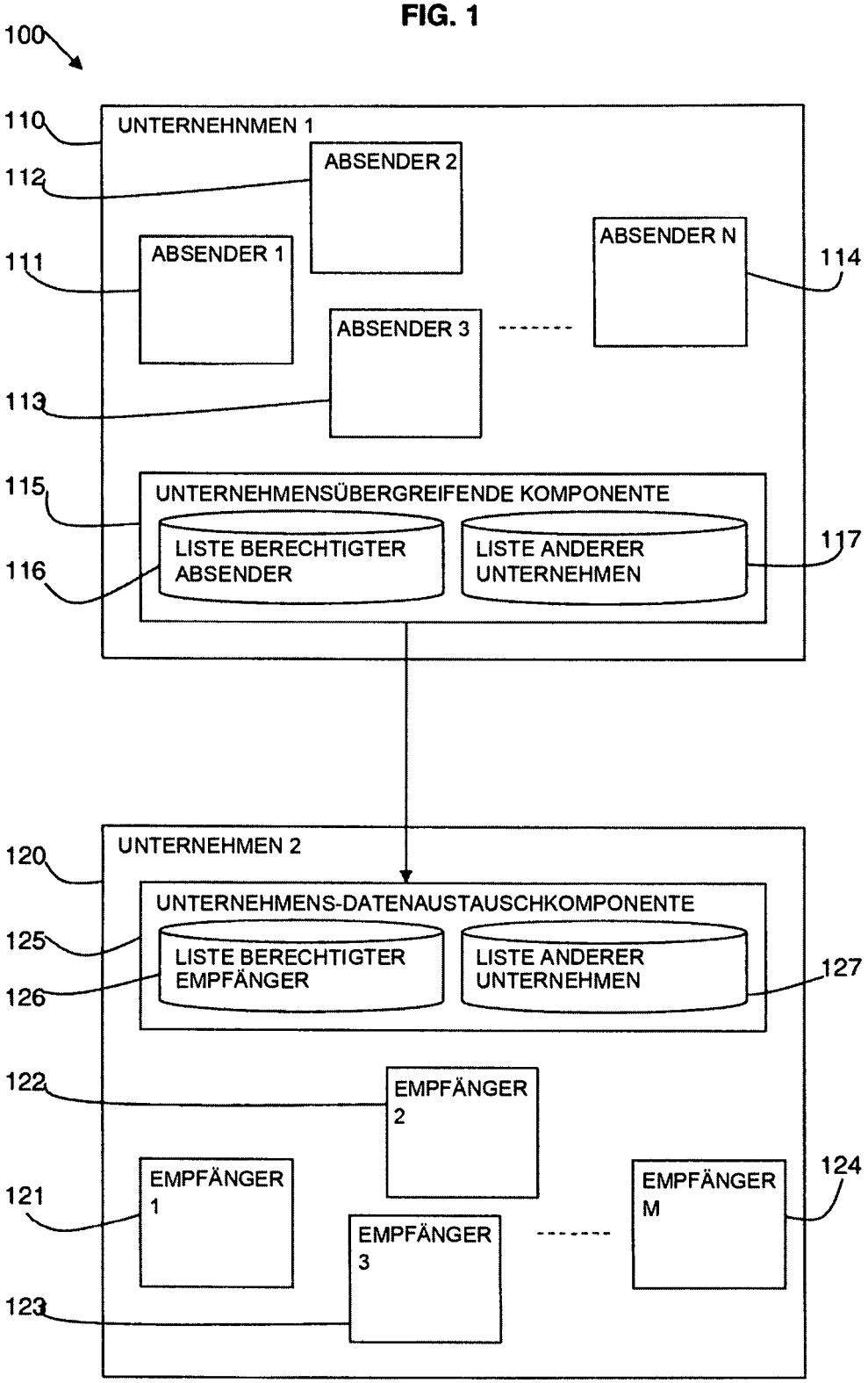


FIG. 2

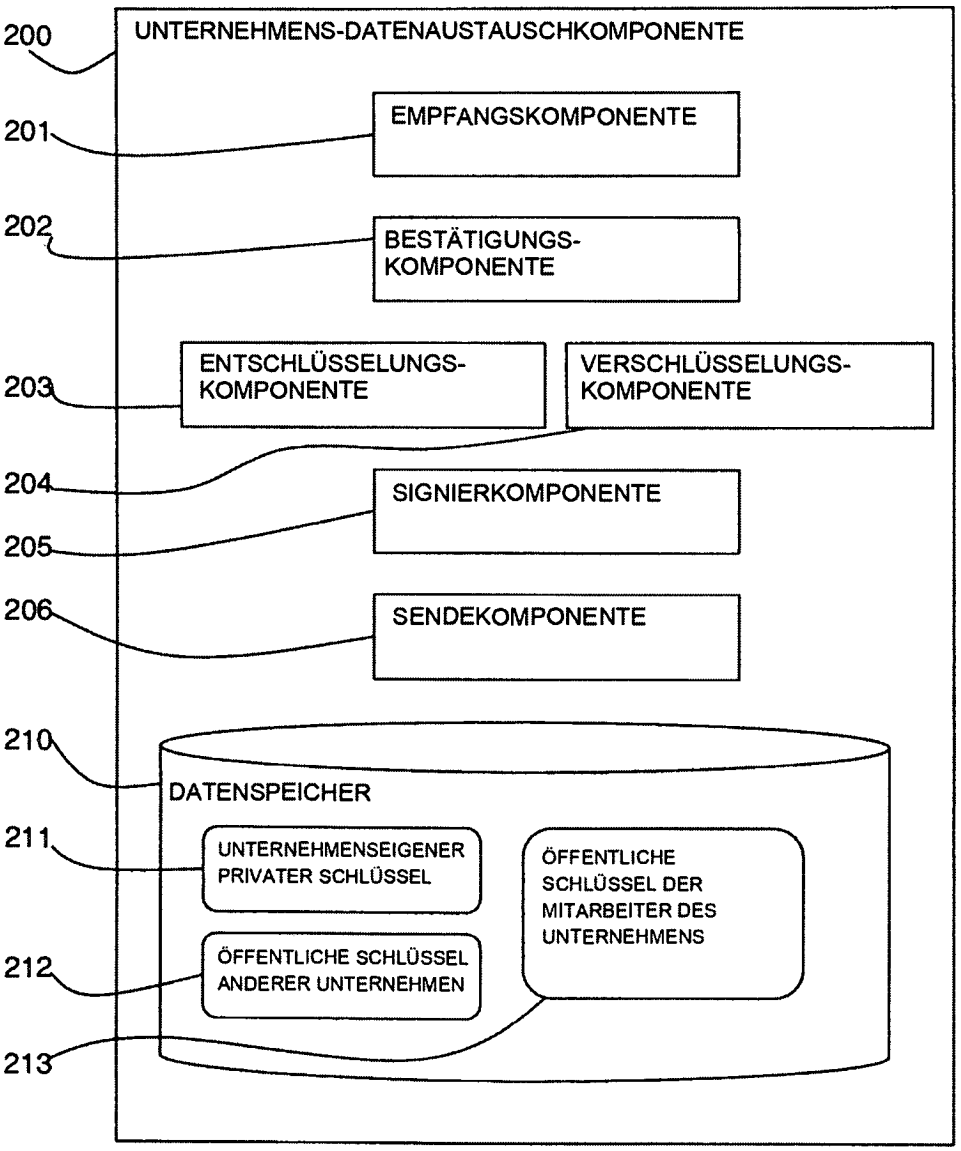

200
UNTERNEHMENS-DATENAUSTAUSCHKOMPONENTE
201
EMPFANGSKOMPONENTE
202
BESTÄTIGUNGS-KOMPONENTE
203
ENTSCHLÜSSELUNGS-KOMPONENTE
VERSCHLÜSSELUNGS-KOMPONENTE
204
SIGNIERKOMPONENTE
205
206
SENDEKOMPONENTE
210
DATENSPEICHER
211
UNTERNEHMENSEIGENER PRIVATER SCHLÜSSEL
ÖFFENTLICHE SCHLÜSSEL DER MITARBEITER DES UNTERNEHMENS
212
ÖFFENTLICHE SCHLÜSSEL ANDERER UNTERNEHMEN
213

FIG. 3

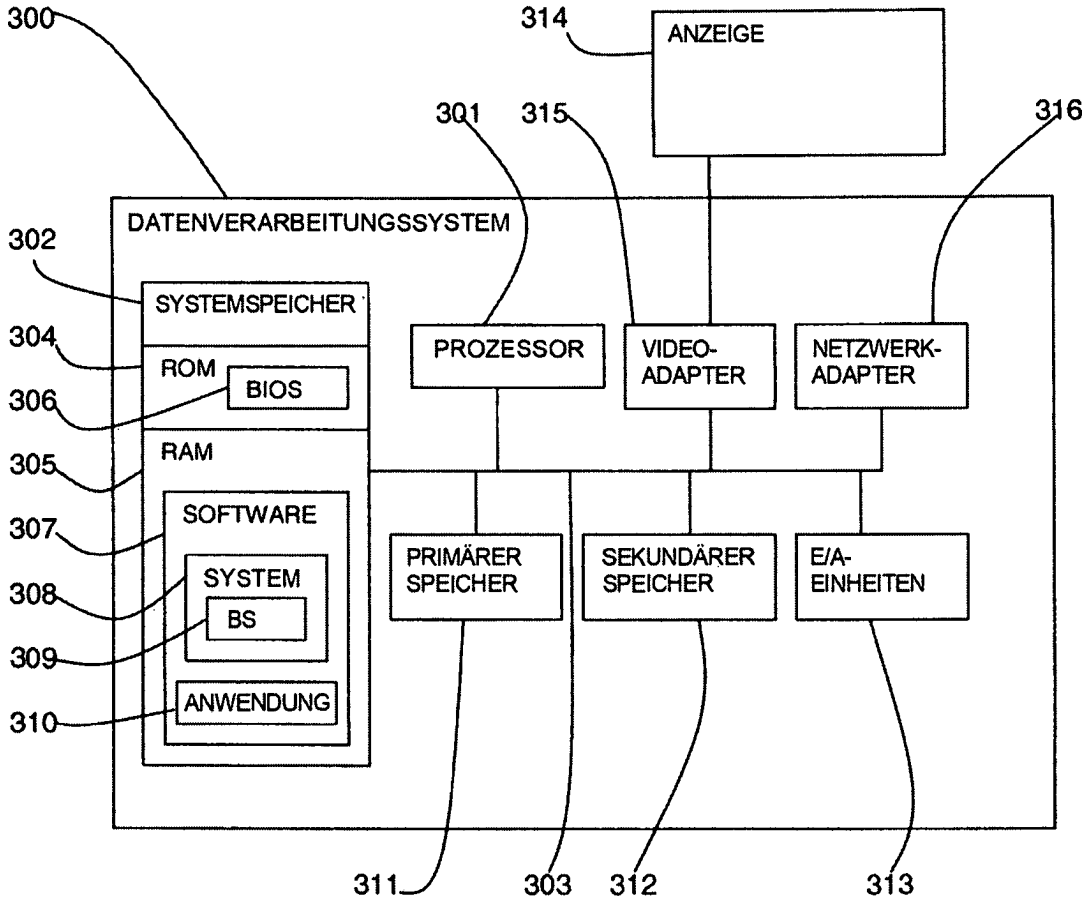

300
314
ANZEIGE
301
315
316
DATENVERARBEITUNGSSYSTEM
302
SYSTEMSPEICHER
304
ROM
BIOS
306
RAM
305
SOFTWARE
307
SYSTEM
308
BS
309
ANWENDUNG
310
PROZESSOR
VIDEO-ADAPTER
NETZWERK-ADAPTER
PRIMÄRER SPEICHER
SEKUNDÄRER SPEICHER
E/A-EINHEITEN
311
303
312
313

FIG. 4A

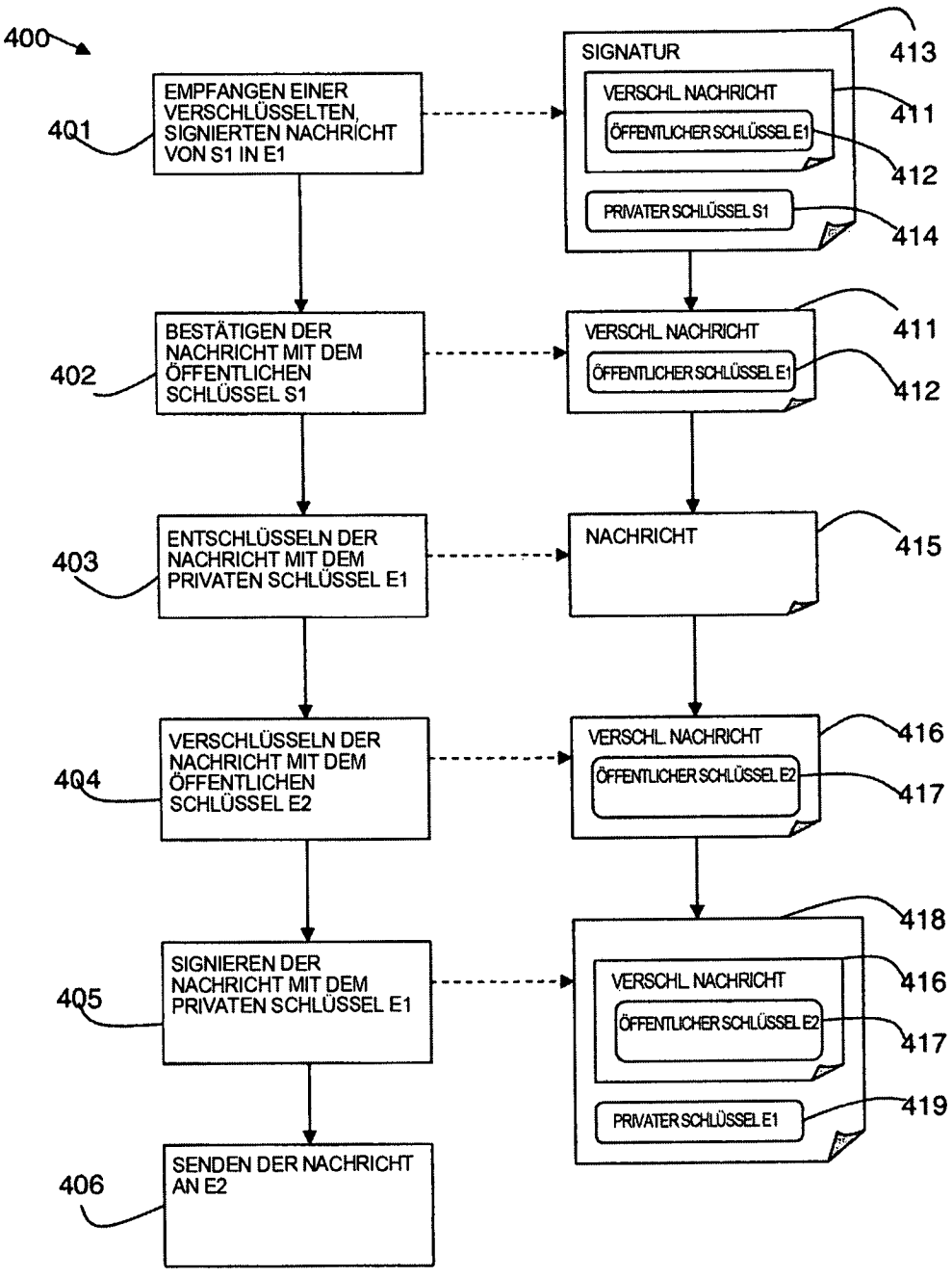

400
401
EMPFANGEN EINER VERSCHLÜSSELTEN, SIGNIERTEN NACHRICHT VON S1 IN E1
402
BESTÄTIGEN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL S1
403
ENTSCHLÜSSELN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E1
404
VERSCHLÜSSELN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL E2
405
SIGNIEREN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E1
406
SENDEN DER NACHRICHT AN E2
SIGNATUR
413
VERSCHL. NACHRICHT
411
ÖFFENTLICHER SCHLÜSSEL E1
412
PRIVATER SCHLÜSSEL S1
414
VERSCHL. NACHRICHT
411
ÖFFENTLICHER SCHLÜSSEL E1
412
NACHRICHT
415
VERSCHL. NACHRICHT
416
ÖFFENTLICHER SCHLÜSSEL E2
417
418
VERSCHL. NACHRICHT
416
ÖFFENTLICHER SCHLÜSSEL E2
417
PRIVATER SCHLÜSSEL E1
419

FIG. 4B

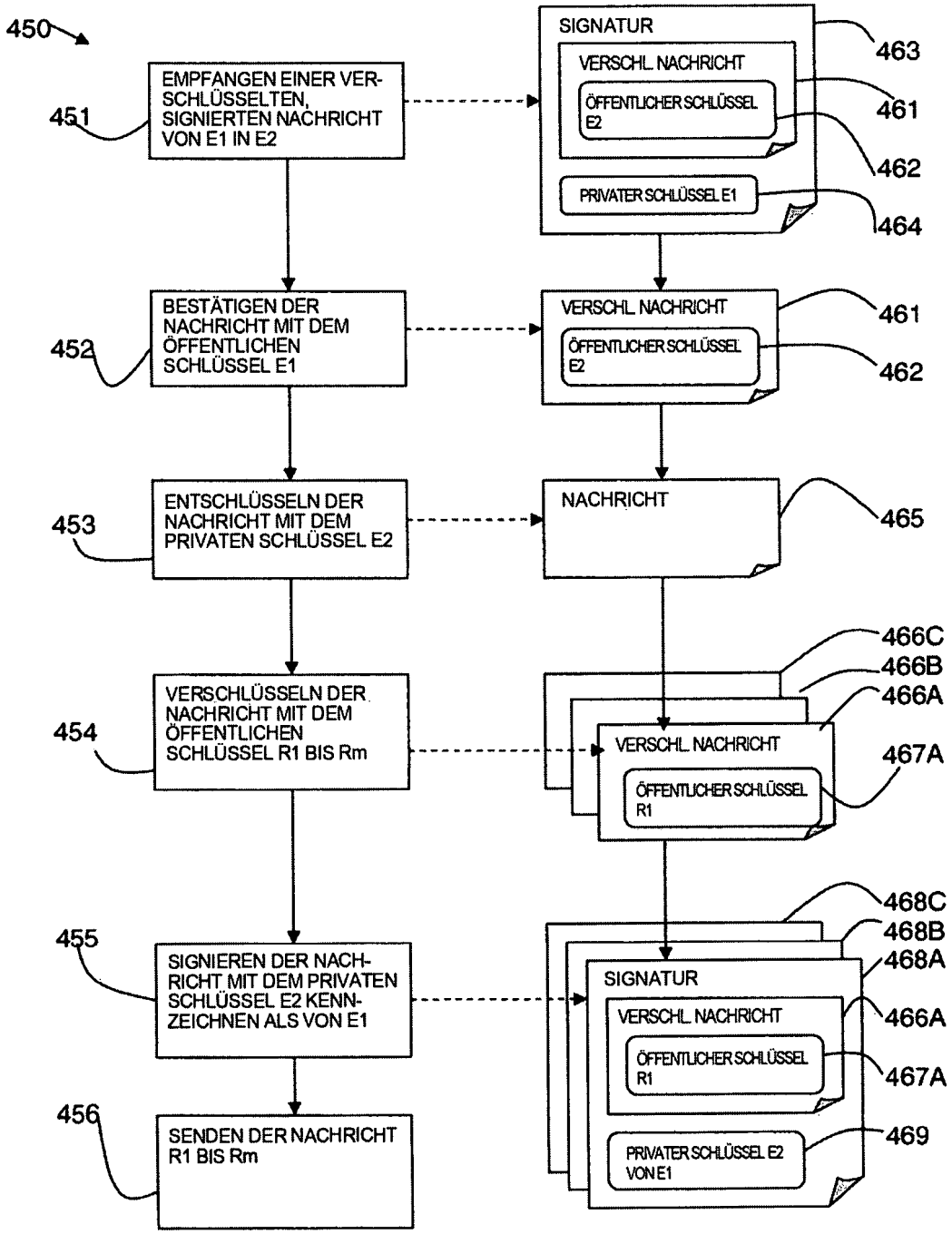

450
451
EMPFANGEN EINER VERSCHLÜSSELTEN, SIGNIERTEN NACHRICHT VON E1 IN E2
452
BESTÄTIGEN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL E1
453
ENTSCHLÜSSELN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E2
454
VERSCHLÜSSELN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL R1 BIS Rm
455
SIGNIEREN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E2 KENNZEICHNEN ALS VON E1
456
SENDEN DER NACHRICHT R1 BIS Rm
SIGNATUR
VERSCHL. NACHRICHT
ÖFFENTLICHER SCHLÜSSEL E2
PRIVATER SCHLÜSSEL E1
463
461
462
464
VERSCHL. NACHRICHT
ÖFFENTLICHER SCHLÜSSEL E2
461
462
NACHRICHT
465
466C
466B
466A
VERSCHL. NACHRICHT
ÖFFENTLICHER SCHLÜSSEL R1
467A
468C
468B
468A
SIGNATUR
VERSCHL. NACHRICHT
ÖFFENTLICHER SCHLÜSSEL R1
466A
467A
PRIVATER SCHLÜSSEL E2 VON E1
469

FIG. 5A

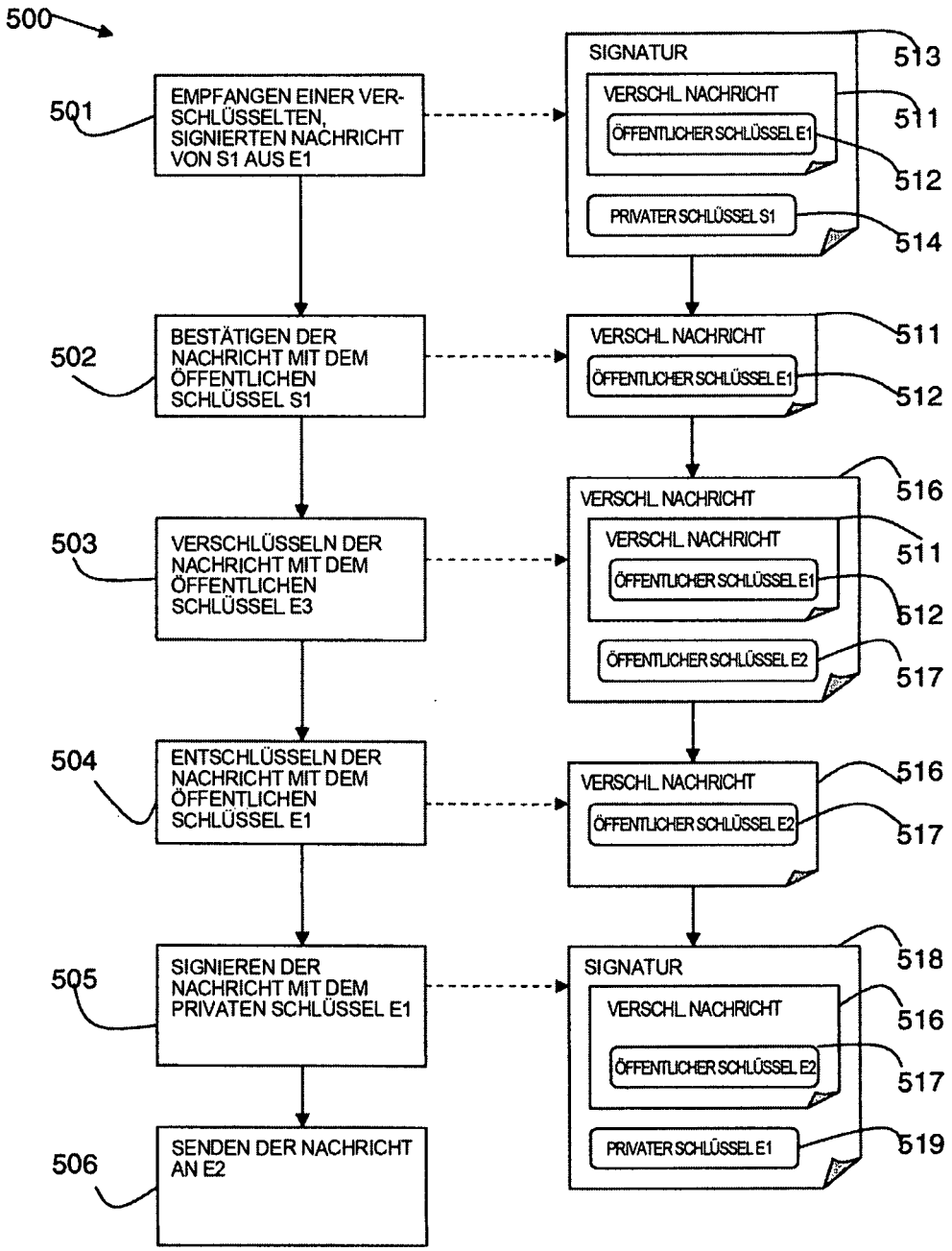
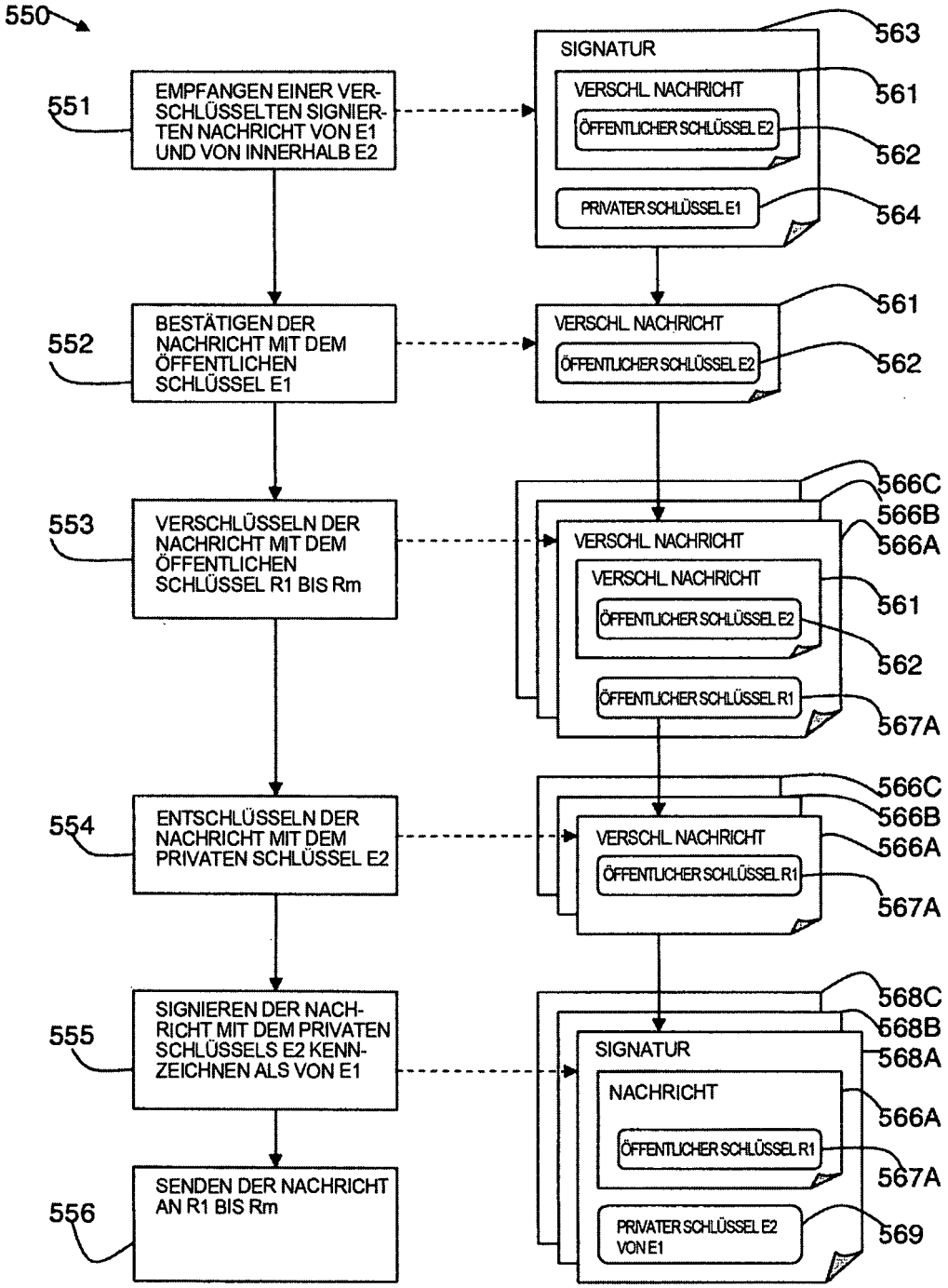

500
501
EMPFANGEN EINER VER-SCHLÜSSELTEN, SIGNIERTEN NACHRICHT VON S1 AUS E1
502
BESTÄTIGEN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL S1
503
VERSCHLÜSSELN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL E3
504
ENTSCHLÜSSELN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL E1
505
SIGNIEREN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E1
506
SENDEN DER NACHRICHT AN E2
SIGNATUR
513
VERSCHL. NACHRICHT
511
ÖFFENTLICHER SCHLÜSSEL E1
512
PRIVATER SCHLÜSSEL S1
514
VERSCHL. NACHRICHT
511
ÖFFENTLICHER SCHLÜSSEL E1
512
VERSCHL. NACHRICHT
516
VERSCHL. NACHRICHT
511
ÖFFENTLICHER SCHLÜSSEL E1
512
ÖFFENTLICHER SCHLÜSSEL E2
517
VERSCHL. NACHRICHT
516
ÖFFENTLICHER SCHLÜSSEL E2
517
SIGNATUR
518
VERSCHL. NACHRICHT
516
ÖFFENTLICHER SCHLÜSSEL E2
517
PRIVATER SCHLÜSSEL E1
519

FIG. 5B


550
551
EMPFANGEN EINER VERSCHLÜSSELTEN SIGNIERTEN NACHRICHT VON E1 UND VON INNERHALB E2
552
BESTÄTIGEN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL E1
553
VERSCHLÜSSELN DER NACHRICHT MIT DEM ÖFFENTLICHEN SCHLÜSSEL R1 BIS Rm
554
ENTSCHLÜSSELN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSEL E2
555
SIGNIEREN DER NACHRICHT MIT DEM PRIVATEN SCHLÜSSELS E2 KENNZEICHNEN ALS VON E1
556
SENDEN DER NACHRICHT AN R1 BIS Rm
SIGNATUR
563
VERSCHL NACHRICHT
561
ÖFFENTLICHER SCHLÜSSEL E2
562
PRIVATER SCHLÜSSEL E1
564
VERSCHL NACHRICHT
561
ÖFFENTLICHER SCHLÜSSEL E2
562
566C
566B
566A
VERSCHL NACHRICHT
VERSCHL NACHRICHT
561
ÖFFENTLICHER SCHLÜSSEL E2
562
ÖFFENTLICHER SCHLÜSSEL R1
567A
566C
566B
566A
VERSCHL NACHRICHT
ÖFFENTLICHER SCHLÜSSEL R1
567A
568C
568B
568A
SIGNATUR
NACHRICHT
566A
ÖFFENTLICHER SCHLÜSSEL R1
567A
PRIVATER SCHLÜSSEL E2 VON E1
569