(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 447 716 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
27.02.2019 Patentblatt 2019/09

(51) Int Cl.:
G06Q 50/00 *(2012.01)*

(21) Anmeldenummer: **17187030.6**

(22) Anmeldetag: **21.08.2017**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
MA MD

(71) Anmelder: **Rinau, André**
67657 Kaiserslautern (DE)

(72) Erfinder:
- **HILDEBRANDT, Anna Katharina**
  66123 Saarbrücken (DE)
- **RINAU, André**
  67657 Kaiserslautern (DE)

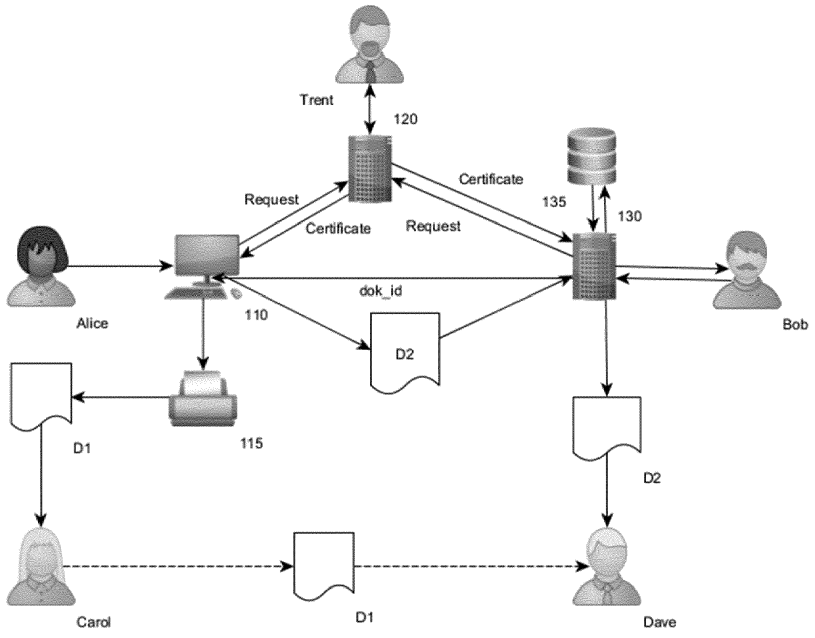
(74) Vertreter: **Bach, Alexander**
Mitscherlich PartmbB
Patent- und Rechtsanwälte
Sonnenstraße 33
80331 München (DE)

(54) **AUTOMATISIERTE VERFAHREN UND VORRICHTUNG ZUR BEGLAUBIGUNG UND VERIFIKATION VON DOKUMENTEN**

(57) Zur Beglaubigung eines Dokuments wird ein computer-implementiertes Verfahren bereitgestellt, umfassend die Schritte:
- Erhalten eines elektronischen Dokuments;
- Kombinieren des elektronischen Dokuments mit einer Dokumentenkennung (ID), um ein überprüfbares Dokument zu erhalten;
- Ausgeben des überprüfbaren Dokuments auf einem Drucker oder über ein Netzwerk.

Gemäß der Erfindung wird das elektronische Dokuments ferner über ein Netzwerk an einen Server übermittelt, wobei der Server über einen Datenspeicher zur Speicherung des elektronischen Dokuments und über eine Schnittstelle zur Bereitstellung des elektronischen Dokuments an Dritte verfügt.

Figur 1



EP 3 447 716 A1

Beschreibung

[0001] Die Erfindung betrifft automatisierte Verfahren zur Beglaubigung und Verifikation von Dokumenten, insbesondere, wenn diese beispielsweise in Papierform in Umlauf gebracht werden.

[0002] Dokumente können heutzutage mit geringem Aufwand und hoher Qualität gefälscht werden. Gefälschte Dokumente können komplett neu erstellt oder in Teilen verändert sein. Fälschungen lassen sich auch mit technischen Methoden häufig nicht mehr als solche identifizieren. Dokumentenfälschung ist daher ein ernsthaftes und zunehmendes Problem, das durch bestehende Rahmenbedingungen verschärft wird. Der Nachweis der Echtheit eines Dokuments ist für Dritte häufig nicht möglich bzw. mit hohem Aufwand verbunden, teilweise nur unter Zuzug von Sachverständigen. Die oft einzige Möglichkeit für Dritte, die Echtheit eines Dokumentes (bzw. einer Kopie) zu verifizieren, ist die Anfrage beim Urheber des Dokuments. Häufig ist dies mit erheblichem Aufwand verbunden, der auch bei begründetem Verdacht häufig vermieden wird. In den meisten Fällen unterliegt der Urheber außerdem Datenschutzvorschriften und darf somit keine Auskunft geben. Insb. Prüfungsämter von Hochschulen, Schulen und Arbeitgeber dürfen ohne Zustimmung des Zeugnisinhabers keine Auskunft über Zeugnisinhalte geben oder das Originalzeugnis oder Auszüge davon weitergeben.

[0003] Als Fälschungsschutz kommen derzeit in Abhängigkeit der Form des Dokuments zwei Lösungen zum Einsatz. Papierbasierte Dokumente können mit physischen Echtheitsverfahren geschützt werden, digitale Dokumente mit digitalen Signaturverfahren.

[0004] Physischen Echtheitsverfahren: Zum Schutz von Dokumenten werden primär optische Sicherheitsmerkmale verwendet wie Wasserzeichen, Spezialpapier, Sicherheitsstreifen, Durchsichtsfenster, fluoreszierende Farben oder Hologramme. Hierbei handelt es sich um von Menschen erkennbare Merkmale. Es werden jedoch auch maschinell erkennbare Merkmale verwendet. Hierzu gehören bspw. Infrarot-Farbe oder magnetische Elemente. Die Anwendung der maschinell erkennbaren Merkmale ist für die meisten Dokumentenurheber keine Option, da zusätzliche Hardware benötigt wird, die teilweise sehr teuer ist. Auch Dritte würden entsprechende Hardware benötigen, um die Merkmale auszulesen und das Dokument verifizieren zu können. Besitzen sie diese Hardware nicht, können sie das Dokument nicht verifizieren. Physische Echtheitsverfahren erschweren das Erstellen einer Fälschung, können eine Fälschung aber nicht sicher verhindern. Heutzutage lassen sich unzureichend geschützte Dokumente mittels konventionellen Reproduktionsgeräten wie bspw. Scannern mit hoher Auflösung, Farbkopierern oder kleinen Druckpressen leicht kopieren und fälschen. Ein sicherer Schutz vor Fälschung kann mit physischen Lösungen nicht erreicht werden. Insbesondere, wenn vom Originaldokument eine digitale oder papierbasierte Kopie erstellt wird, ist der physische Schutz nicht mehr vorhanden.

[0005] Digitale Signaturverfahren schützen ausschließlich digitale Dokumente. Sie gewährleisten, dass der Absender der Daten authentisch ist und die digital verschickten Daten nicht verändert wurden und damit unverfälscht sind.

[0006] Beglaubigungen sind keine Lösung der Fälschungsproblematik, vielmehr verschärfen sie das Grundproblem. Grundsätzlich ist eine Beglaubigung nur eine Bescheinigung, dass eine Zweitschrift/Kopie mit einem vorgelegten Schriftstück übereinstimmt. Die Urkundspersonen sind in der Regel nicht die Urheber des Dokuments. Die Frage, ob das vorgelegte Dokument ein Original ist, wird im Rahmen der Beglaubigung nicht beantwortet. Die Bestimmung der Echtheit des vorgelegten Dokuments ist auch den Urkundspersonen aus geschilderten Gründen in der Regel nicht möglich. Tatsächlich verschärft dies die Problematik weiter, da Beglaubigungen von Fälschungen im Grunde problemlos möglich sind. So entstehen beglaubigte Kopien von Fälschungen, deren Echtheit nicht mehr hinterfragt wird.

[0007] Aufgabe der vorliegenden Erfindung ist daher, automatisierte Verfahren und Vorrichtung bereit zu stellen, welche einen einfachen und sicheren Schutz vor gefälschten Dokumenten ermöglichen. Verhindert werden soll eine Fälschung bzw. Manipulation durch die Inhaber der Dokumente oder Dritte (bspw. Arbeitszeugnisse, Abschlusszeugnisse, Zertifikate) sowie eine nachträgliche Manipulation durch den Urheber (bspw. nachträgliche Änderung von Zeugnissen oder Verträgen).

[0008] Diese Aufgabe wird gelöst durch die Verfahren und Vorrichtungen gemäß der unabhängigen Patentansprüche. Vorteilhafte Ausführungsformen sind in den abhängigen Patentansprüchen definiert.

[0009] In einem ersten Aspekt stellt die Erfindung ein computer-implementiertes Verfahren zur Beglaubigung eines Dokuments bereit, umfassend die Schritte: Erzeugen eines elektronischen Dokuments; Versehen des elektronischen Dokuments mit einer digitalen Signatur, um ein signiertes Dokument zu erhalten; Senden des signierten Dokuments an einen Datenspeicher, um einen Abruf durch Dritte zu ermöglichen; Kombinieren des elektronischen Dokuments mit einer Dokumentenkennung, um ein überprüfbares Dokument zu erhalten; und Ausgeben des überprüfbaren Dokuments. Gemäß der Erfindung werden hierdurch zwei Versionen desselben Dokuments hergestellt: ein mit einer Dokumentenkennung versehenes Original, welches in elektronischer oder in Papierform in Verkehr gebracht werden kann, sowie ein zum Abruf durch Dritte bei einer Hinterlegungsstelle gespeichertes Überprüfungsexemplar, welches erforderlichenfalls zur Überprüfung eines Originals durch Vergleich der Inhalte der beiden Dokumente herangezogen werden kann. Die Authentizität des Überprüfungsexemplars wird durch die digitale Signatur des Erstellers gewährleistet; eine Signatur des Originals ist nicht mehr erforderlich, an ihre Stelle tritt das Aufbringen der Dokumentenkennung, welche das Überprüfungsexemplar

identifiziert.

[0010] Um zu verhindern, dass die Hinterlegungsstelle Kenntnis vom Inhalt des Dokuments erlangt, kann das signierte Dokument zusätzlich verschlüsselt werden. Um einem Dritten die Überprüfung eines Originals zu erleichtern, kann das Original neben der Dokumentenkennung auch mit einem Schlüssel zum Entschlüsseln des verschlüsselten Überprüfungsexemplars versehen werden. Die Ver- und Entschlüsselung kann zur Vereinfachung mit einem symmetrischen Schlüssel erfolgen, ohne eine etwaige Vertraulichkeit des Dokuments zu beeinträchtigen, die auch bei Verwendung eines symmetrischen Schlüssels gewährleistet ist, solange nur befugte Stellen von diesem Kenntnis erlangen. Insbesondere ist der Schlüssel nicht zum Abruf des Überprüfungsexemplars bei der Hinterlegungsstelle erforderlich, sondern die Hinterlegungsstelle kann - automatisiert - so betrieben werden, dass ein Abruf über die Dokumentenkennung ermöglicht wird.

[0011] Das Kombinieren des elektronischen Dokuments mit der Dokumentenkennung kann durch Aufbringen der Dokumentenkennung auf dem elektronischen Dokument erfolgen. Die Dokumentenkennung kann in maschinenlesbarer Form aufgebracht werden, beispielsweise als graphischer Code, welcher die Dokumentenkennung repräsentiert.

[0012] In einem zweiten Aspekt stellt die Erfindung ein computer-implementiertes Verfahren zur Verwaltung von Dokumenten bereit, umfassend die Schritte: Erzeugen einer ersten Dokumentenkennung (ID1); Empfangen eines elektronischen Dokuments von einem Nutzer, wobei das elektronische Dokument von diesem digital signiert ist; Speichern des elektronischen Dokuments in einem nichtflüchtigen Speicher, unter der ersten Dokumentenkennung (ID1); Empfangen einer zweiten Dokumentenkennung (ID2); Bereitstellen des elektronischen Dokuments, wenn die erste Dokumenten-kennung (ID1) der zweiten Dokumentenkennung (ID2) entspricht.

[0013] Um einem Nutzer zu erlauben, die Identität der Hinterlegungsstelle für ein Überprüfungsdokument zu verifizieren, kann dem elektronischen Dokument eine digitale Signatur hinzugefügt werden. Um zu verhindern, dass der Empfänger vom Inhalt des elektronischen Dokuments Kenntnis nimmt, kann das empfangene elektronische Dokument verschlüsselt sein. Die Verschlüsselung kann mit einem symmetrischen Schlüssel erfolgen.

[0014] Die verwendete Dokumentenkennung kann zunächst von einem Nutzer angefordert worden sein. Die Anforderung der Dokumentenkennung kann von dem Nutzer digital signiert worden oder über einen authentifizierten Kanal verschickt worden sein. Um sicherzustellen, dass sich kein Dritter als ein bestimmter Nutzer ausgibt, kann die Signatur der Anforderung verifiziert und gegebenenfalls zurückgewiesen werden. Bei Erfolg kann die erzeugte Dokumentenkennung an den Nutzer verschickt werden. Die Dokumentenkennung eines eingehenden elektronischen Dokuments kann mit der erzeugten Dokumentenkennung verglichen werden, um zu gewährleisten, dass ein Nutzer eine zulässige Dokumentenkennung verwendet, beispielsweise um eine eindeutige Zuordnung von Dokumenten und Kennungen auf Seiten der Hinterlegungsstelle zu gewährleisten. Umgekehrt kann auch die versandte Dokumentenkennung digital signiert werden, um dem anfordernden Nutzer zu erlauben, die Identität des Ausstellers der Dokumentenkennung zu verifizieren. Außerdem kann die Dokumentenkennung verschlüsselt werden, um einen Missbrauch derselben durch unbefugte Dritte zu verhindern.

[0015] Diese und weitere Aspekte der vorliegenden Erfindung werden nachstehend anhand eines konkreten Ausführungsbeispiels erläutert, unter Bezugnahme auf die anliegende Zeichnung, in welcher

Figur 1 eine schematische Übersicht über das Zusammenwirken der einzelnen Verfahren gemäß einer Ausführungsform der Erfindung zeigt;

Figur 2 Vorbereitungen zum Einsatz der Verfahren gemäß einer Ausführungsform der Erfindung zeigt;

Figur 3 die Dokumentenerzeugung und -übertragung gemäß einer Ausführungsform der Erfindung zeigt;

Figur 4 die Dokumentensignierung gemäß einer Ausführungsform der Erfindung zeigt, und

Figur 5 die Dokumentenverifikation gemäß einer Ausführungsform der Erfindung zeigt.

[0016] Figur 1 zeigt eine schematische Übersicht über die einzelnen Verfahren und ihr Zusammenwirken gemäß einer Ausführungsform der Erfindung.

[0017] Die Rollen der einzelnen Teilnehmer der gegenständlichen Verfahren sind dabei entsprechend der üblichen kryptographischen Namensgebung benannt. Bob bietet einen Cloudbasierten Dienst zum Speichern und Verifizieren von Dokumenten an. Ihm darf zu keinem Zeitpunkt Dokumenteninhalt oder Schlüssel zur Verfügung gestellt werden, jedenfalls wenn Verschlüsselung verwendet wird. Alice möchte Dokumente zur Verifikation verschlüsselt in der Cloud ablegen, darf Geheimnisse dieses bestimmten Dokuments (d.h. Dokumenteninhalt und Schlüssel) kennen. Trent betreibt eine zentrale Zertifizierungsstelle Alle Protokollteilnehmer vertrauen Trent (verwendet als Stammzertifizierungsstelle). Carol möchte ihre Dokumente bei Dave zur Verifikation einreichen. Dave vertraut nicht darauf, dass sie die korrekte Originalversion der Dokumente einreicht. Dave möchte Carols Dokumente daher verifizieren. Carol vertraut ihm den Inhalt und den Schlüssele zu genau diesen Dokumenten an.

[0018] Alice verwendet einen Rechner 110 um ein Originaldokument D2 zu erstellen und versendet dieses ei-

nerseits mit seiner digitalen Signatur versehen an eine Hinterlegungsstelle 130, die von Bob betrieben wird, welche das Dokument mit einer Kennung versehen speichert und zum Abruf durch Dritte 120 unter dieser Dokumentenkennung bereit hält. Sodann erzeugt Alice eine mit der Dokumentenkennung versehenen Ausdruck des Originals D1 auf einem Drucker 115 und bringt diesen in Umlauf. Um die Echtheit des Dokuments zu überprüfen, kann Dave mittels der auf dem Originalausdruck aufgebrachten Dokumentenkennung die hinterlegte und digital signierte Kopie des Originals bei der Hinterlegungsstelle 130 abrufen und sowohl die Signatur von Alice als auch den Inhalt des Dokuments verifizieren, um Fälschungen auszuschließen.

[0019] Die Überprüfung von Dokumenten aus Nutzerperspektive erfolgt dabei gemäß einer Ausführungsform der Erfindung in folgenden Schritten:

» Eingang des Dokuments: Der Nutzer erhält ein verifizierbares Dokument im Original, als papierbasierte Kopie (bspw. per Post oder persönlich) oder eine digitale Kopie (bspw. per E-Mail oder Online-Bewerberportal).

» Alternative 1:

Der Nutzer scannt den QR-Code mit einem QR Code Reader. Dem Nutzer wird das Originaldokument auf seinem End-gerät angezeigt. Er kann es nun mit der ihm vorliegenden Fassung vergleichen.

» Alternative 2:

Der Nutzer besucht die Web-Seite des Anbieters und wählt ein lokal gespeichertes digitales Dokument aus (ggf. vorherige Umwandlung eines Papierdokuments in digitales Dokument). Dem Nutzer wird das zu dem gewählten Dokument gehörige Originaldokument angezeigt. Auf Wunsch kann er es automatisiert mit dem hochgeladenen Dokument vergleichen. Aus Datenschutzgründen wird dabei das zu prüfende Dokument nicht über das Internet übertragen, sondern vollständig auf dem Nutzer-Rechner mit Hilfe von JavaScript verarbeitet (QR-Code Detektion, Anfrage nach verschlüsseltem Originaldokument, Entschlüsseln).

» Die Installation des Add-Ins kann dabei nach Download aus dem Internet erfolgen.

[0020] Im verwendeten Verifikationsprotokoll ist sichergestellt, dass der Anbieter (im Protokoll entsprechend der Literatur im Gebiet IT-Sicherheit als «Bob» bezeichnet) zu keinem Zeitpunkt Dokumenteninhalte einsehen kann, da der verwendete Key nicht übertragen wird, Bob nicht bekannt ist und auch in keiner Datenbank gespeichert ist.

[0021] Der Key befindet sich (in Form eines QR-Codes) nur auf dem Dokument. Schlüsselerstellung und Verschlüsselung erfolgen vollständig auf dem Client, nicht auf dem Server. Nur Personen, die das Dokument (oder eine Kopie des Dokuments) physisch oder digital erhalten haben, können das Originaldokument verifizieren (einsehen). Dabei gelangt der Schlüssel nicht in die Cloud. Die Entschlüsselung erfolgt erst auf dem Nutzer-Rechner, nachdem das Dokument verschlüsselt heruntergeladen wurde.

[0022] Figur 2 zeigt Vorbereitungen zum Einsatz der Verfahren gemäß einer Ausführungsform der Erfindung.

[0023] Bob erzeugt ein zufälliges Public/Private Key-Paar. Er konkateniert seinen Namen mit dem Public Key und lässt Trent das Key/Name-Paar mit dessen Private Key signieren.

[0024] Alice erzeugt ein zufälliges Public/Private Key-Paar. Sie konkateniert ihren Namen mit dem Public Key und lässt Trent das Key/Name Paar mit dessen Private Key signieren. Dann lädt sie Bob's Public Key/Name-Paar herunter, überprüft Trent's Signatur und extrahiert Bob's Public Key. Mit diesem verschlüsselt sie ihr Public Key/Name-Paar und schickt diese Informationen zu Bob. Bob entschlüsselt das empfangene Public Key/Name-Paar mit seinem privaten Schlüssel und überprüft Trent's Signatur. Dann extrahiert er das Public Key/Name Paar von Alice, signiert es mit seinem private Key, verschlüsselt das Public Key/Name-Paar mit dem Public Key von Alice und schickt ihr diese Information.

[0025] Figur 3 zeigt ein Verfahren zur Dokumentenerzeugung und -übertragung gemäß einer Ausführungsform der Erfindung.

[0026] Das erfindungsgemäße Verfahren kann als Web-Service implementiert werden. Hierfür sind zwei Komponenten vorgesehen. Der Dokumentenschutz wird mit einer Desktop-Applikation oder einem Drucker Add-in vorgenommen, die Verifikation erfolgt Webbasiert.

[0027] Der Schutz eines Dokuments aus Nutzerperspektive erfolgt dabei gemäß einer Ausführungsform der Erfindung in folgenden Schritten:

» Schritt 1: Dem Nutzer steht eine Desktop-Applikation zur Verfügung:

» Schritt 3: Der Nutzer meldet sich mit Benutzername und Kennwort an. Beides hat er im Rahmen des Registrierungsprozesses erhalten bzw. festgelegt.

» Schritt 4: Der Nutzer wählt das zu schützende Dokument in der lokalen Ablage aus, legt die Position des QR-Codes auf dem Dokument und einen Untertitel fest (bspw. «Dieses Dokument kann durch Einlesen des QR-Codes auf Website "Platzhalter" verifiziert werden»). Für Position und Untertitel kann der Nutzer Standards definieren.

» Schritt 5: Der Nutzer klickt «Dokument schützen»:

QR-Code und Untertitel werden automatisch auf dem Dokument aufgebracht, das Dokument wird verschlüsselt hochgeladen (vergleiche Verifikationsprotokoll) und auf dem vorherigen Speicherort schreibgeschützt in PDF-Format gespeichert. Dokumente können nun wie gewohnt weiterverwendet werden (ausdrucken, versenden etc.)

[0028] Figur 4 zeigt ein Verfahren zur Dokumentenverschlüsselung gemäß einer Ausführungsform der Erfindung.

410. Alice erzeugt ein Dokument, das sie schützen möchte. Alice besitzt ein Zertifikat (cert), das in der Vorbereitungsphase erzeugt wurde, und einen privaten Schlüssel zum Unterschreiben sk.

420. Sie erzeugt einen zufälligen Hash-Key (hk) und benutzt diesen, um einen symmetrischen Schlüssel (kc) und eine eindeutige ID (uid) zu erzeugen, unter Verwendung einer Schlüsselerzeugungsfunktion KDF (uid := KDF(hk, "id"), kc := KDF(hk, "kc"). KDF(hk, x) erzeugt einen Hash-Wert aus dem Hash-Key hk und der Eingabe x. KDF ist eine sichere pseudozufällige Funktion, z.B. HKDF-Expand (RFC 5869).

430. Alice erzeugt einen symmetrischen Schlüssel ks und berechnet dann einen symmetrischen Schlüssel k für das Dokument mit einer bitweisen XOR Operation (k := kc XOR ks).

440. Alice verschlüsselt das Dokument mit dem symmetrischen Schlüssel k, um einen verschlüsselten Text c zu erhalten.

450. Alice erzeugt einen Hash-Wert h aus dem verschlüsselten Text c mit k unter Verwendung einer Hash-Funktion H. H ist eine kryptographische Hash-Funktion, z.B. SHA-3 (h := H(k ‖ c), wobei das Symbol ‖ die Konkatenation von Bitstrings bezeichnet.

460. Alice erzeugt eine Signatur mit dem Hash-Wert h und dem privaten Schlüssel sk (s := Sign(sk, h)). Sign(sk, m) ist eine Funktion, die eine Signatur s für eine Nachricht m erzeugt.

470. Alice schickt ihre Information zu dem Server von Bob. Sie schickt (uid, cert, ks, s) an den Server 1 und (uid, c) an den Server 2. Wenn auf einem der Server bereits ein Tuple gespeichert ist, welches uid enthält, wird das Verfahren abgebrochen. Wenn kein Tuple existiert, das uid enthält, wird das geschickte Tuple gespeichert.

480. Alice erzeugt einen QR-Code (qr), der hk enthält.

490. Alice hängt dann qr an das Dokument an und übergibt oder übermittelt es an Carol, in Papier- oder Digitalformat.

[0029] Figur 5 zeigt ein Verfahren zur Dokumentenverifikation gemäß einer Ausführungsform der Erfindung.

510. Carol gibt Dave ein Dokument mit einem QR-Code qr. Dave möchte verifizieren, ob das Dokument authentisch ist.

520. Dave extrahiert den Hash-Key hk aus qr.

530. Dave verwendet KDF um die uid aus hk zurückzugewinnen (uid := KDF(hk, "id").

540. Mit der uid fragt Dave Bobs Server parallel ab, um ihm die gespeicherten Tuple zur Verfügung zu stellen. Wenn kein Tuple in den Datenbanken auf einem der beiden Server vorhanden ist, wird das Verfahren abgebrochen. Wenn Tuple mit uid auf beiden Servern gespeichert sind, erhält Dave (ks, s, cert) von Server 1 und dem verschlüsselten Text c von Server 2.

550. Dave extrahiert nun den öffentlichen Verifikationsschlüssel (vk) von Alice und ihre Identität (A) aus cert und verifiziert, dass das Zertifikat valide ist. Er überprüft, ob cert von einer vertrauenswürdigen Partei ausgegeben wurde (Trent), ob cert vk mit A verbindet und es auch im übrigen valide ist (korrekte Signaturen etc.).

560. Dave erzeugt den symmetrischen Schüssel kc aus hk mit der KDF Hash-Funktion (kc := KDF(hk, "kc").

570. Dann generiert Dave den symmetrischen Schlüssel aus kc und ks unter Verwendung einer bitweisen XOR Operation (k := kc XOR ks).

580. Dann erzeugt Dave einen Hash-Wert h aus k und c (h := H(k ‖ c)).

590. Dave verwendet eine Verifikationsfunktion, um zu überprüfen, ob die Signatur s eine valide Signatur auf h unter vk ist. Verify(vk, h, s) gibt den Wert wahr aus, genau dann wenn es eine valide Signatur auf Nachricht m unter dem öffentlichen Verifikationsschlüssel vk ist. Wenn verify(vk, h, s) den Wert falsch zurückgibt, wird das Verfahren abgebrochen.

595. Dave entschlüsselt den verschlüsselten Text c mit dem symmetrischen Schlüssel k.

599. Dann führt Dave einen (visuellen oder digitalen) Vergleich durch, um zu verifizieren, dass das Dokument, welches er von Carol erhalten hat, sich nicht

von dem Dokument unterscheidet, dass er in dem vorhergehenden Schritt entschlüsselt hat. Wenn der Vergleich nicht erfolgreich wird, bricht Dave ab. Anderenfalls war die Verifikation erfolgreich und das Dokument ist authentisch.

[0030] Zusammenfassend lösen die erfindungsgemäßen Verfahren das Fälschungsproblem damit, dass es Dritten ermöglichen wird, ein vorgelegtes Dokument auf dessen Echtheit zu überprüfen. Bei der Verifikation kann ein automatisierter Abgleich von Dokumenten vorgesehen werden.

[0031] Gegenüber bestehenden Verfahren bieten die Verfahren Sicherheit, dass es sich bei einem vorliegenden Dokument um keine Fälschung handelt. Gleichzeitig sind mit der erfindungsgemäßen Lösung alle digitalen und papierbasierten Kopien der Dokumente gegen Fälschung geschützt. In den meisten Fällen werden Dokumente in Papierform übergeben. Hier helfen digitale Signaturen nicht. Werden Dokumente in digitaler Form übergeben, sind mit der erfindungsgemäßen Lösung auch spätere Papier-Ausdrucke gegen Fälschung geschützt. Zusätzlich ersetzt die erfindungsgemäße Lösung Beglaubigungen, mit entsprechender Aufwandsersparnis für Dokumenteninhaber. Datenschutz ist gewährleistet: Das Dokument kann nur verifizieren, wem es im Original oder als Kopie vorliegt; Die Hinterlegungsstelle oder Dritte haben aufgrund des erfindungsgemäßen Verifikationsprotokolls zu keinem Zeitpunkt Zugriff auf das Dokument. Ein Eingriff in den Verifikationsablauf von außen wird durch die Verwendung geeigneter Zertifikat-Strukturen verhindert. Das erfindungsgemäße Verfahren erlaubt eine Web-basierte Verifizierung, die auf allen gängigen Endgeräten und Browsern möglich ist. Ferner ist der Schutz von Dokumenten aller Formate möglich. Optional kann im Rahmen der Verifizierung ein automatisierter Dokumentenabgleich erfolgen. Bestehende Prozesse beim Dokumentenurheber werden kaum verändert. Das Hochladen und das Abrufen des Dokuments erfolgt bei üblichen Dokumentgrößen unter einer Sekunde, ebenso wie das Schützen und Verifizieren des Dokuments.

Patentansprüche

1. Computer-implementiertes Verfahren zur Beglaubigung eines Dokuments, umfassend die Schritte:

   - Erhalten eines elektronischen Dokuments;
   - Übermitteln des elektronischen Dokuments über ein Netzwerk an einen Server, wobei der Server über einen Datenspeicher zur Speicherung des elektronischen Dokuments und über eine Schnittstelle zur Bereitstellung des elektronischen Dokuments an Dritte verfügt;
   - Kombinieren des elektronischen Dokuments mit einer Dokumentenkennung (ID), um ein überprüfbares Dokument zu erhalten;
   - Ausgeben des überprüfbaren Dokuments auf einem Drucker oder über ein Netzwerk.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** das elektronische Dokument mit einer digitalen Signatur versehen wird, um ein signiertes Dokument zu erhalten, welches an den Server übermittelt wird.

3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet, dass** das signierte Dokument außerdem verschlüsselt wird.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, dass** die Verschlüsselung mit einem symmetrischen Schlüssel erfolgt.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** zusätzlich der symmetrische Schlüssel mit dem elektronischen Dokument kombiniert wird, um das überprüfbare Dokument zu erhalten.

6. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** das Kombinieren des elektronischen Dokuments mit der Dokumentenkennung durch Aufbringen der Dokumentenkennung auf dem elektronischen Dokument erfolgt.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die Dokumentenkennung in maschinenlesbarer Form aufgebracht wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** die maschinenlesbare Form einen graphischen Code (QR) umfasst, welcher die Dokumentenkennung repräsentiert.

9. Verfahren nach Anspruch 2, **dadurch gekennzeichnet, dass** das signierte Dokument über die Dokumentenkennung (ID) aus dem Datenspeicher abrufbar ist.

10. Druckertreiber, der, wenn er auf einem Computer ausgeführt wird, die Schritte des Verfahrens gemäß Anspruch 1 durchführt.

11. Computer-implementiertes Verfahren zur Verwaltung von Dokumenten, umfassend die Schritte:

    - Erhalten einer ersten Dokumentenkennung (ID1);
    - Empfangen eines elektronischen Dokuments von einem ersten Nutzer, wobei das elektronische Dokument von diesem digital signiert ist;
    - Speichern des elektronischen Dokuments in einem nichtflüchtigen Datenspeicher, unter der

ersten Dokumentenkennung (ID1);
- Empfangen einer zweiten Dokumentenkennung (ID2) von einem zweiten Nutzer;
- Bereitstellen des elektronischen Dokuments über eine Schnittstelle an den zweiten Nutzer, wenn die erste Dokumentenkennung (ID1) der zweiten Dokumentenkennung (ID2) entspricht.

12. Verfahren nach Anspruch 11, ferner umfassend den Schritt:

- Hinzufügen einer digitalen Signatur zu dem elektronischen Dokument.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, dass** das empfangene elektronische Dokument verschlüsselt ist.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet, dass** das elektronische Dokument mit einem symmetrischen Schlüssel verschlüsselt ist.

15. Verfahren nach Anspruch 11, ferner umfassend die Schritte:

- Erhalten einer Anforderung einer Dokumentenkennung von dem Nutzer;
- Erhalten der ersten Dokumentenkennung (ID1) durch Erzeugen der ersten Dokumentenkennung (ID1); und
- Senden der ersten Dokumentenkennung (ID1) an den Nutzer.

16. Verfahren nach Anspruch 15, **dadurch gekennzeichnet, dass** die Anforderung einer Dokumentenkennung von dem Nutzer digital signiert ist.

17. Verfahren nach Anspruch 16, ferner umfassend den Schritt:

- Überprüfen der digitalen Signatur des Nutzers.

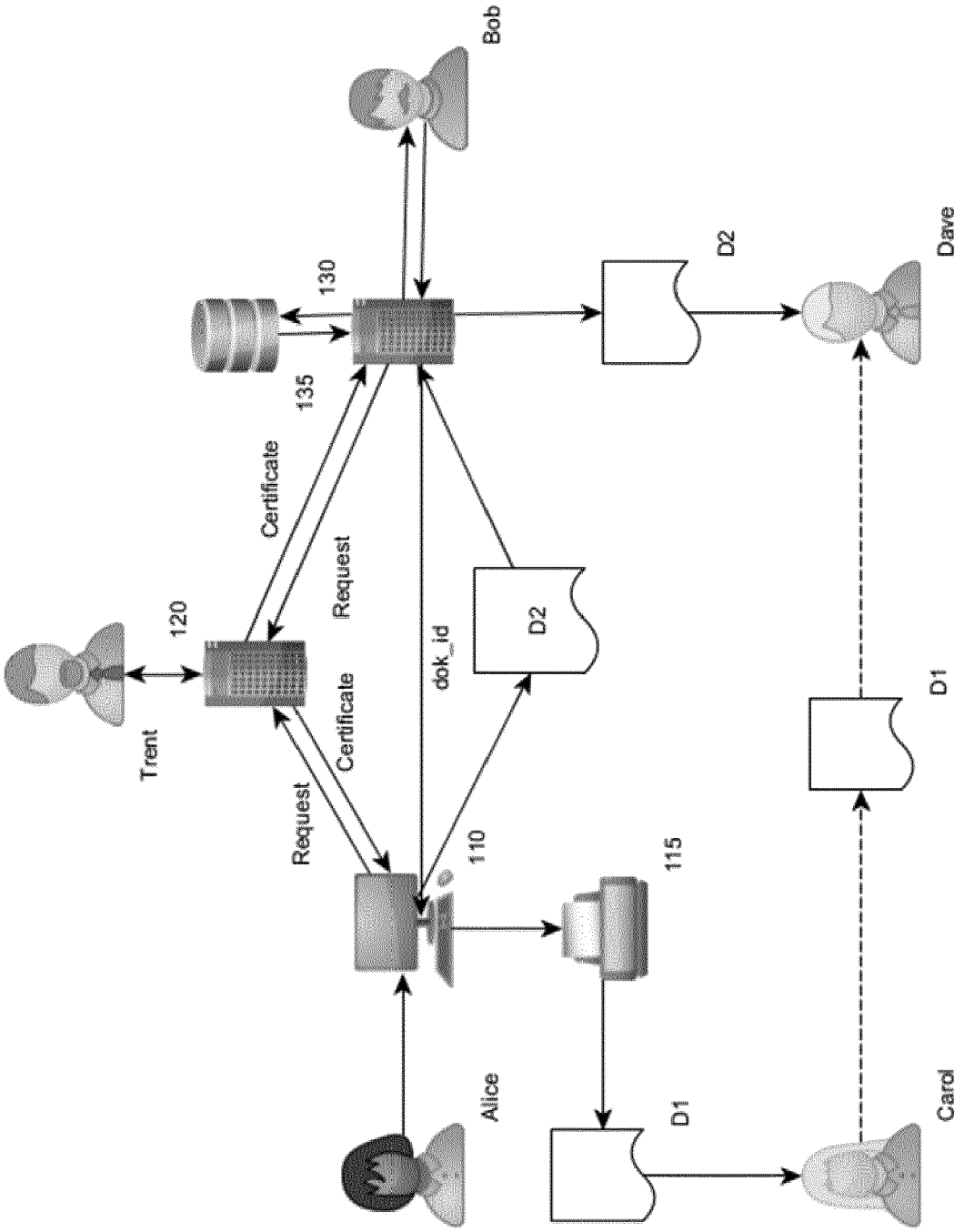
18. Verfahren nach Anspruch 16, ferner umfassend den Schritt:

- digitales Signieren der ersten Dokumentenkennung (ID1) vor dem Versenden an den Nutzer.

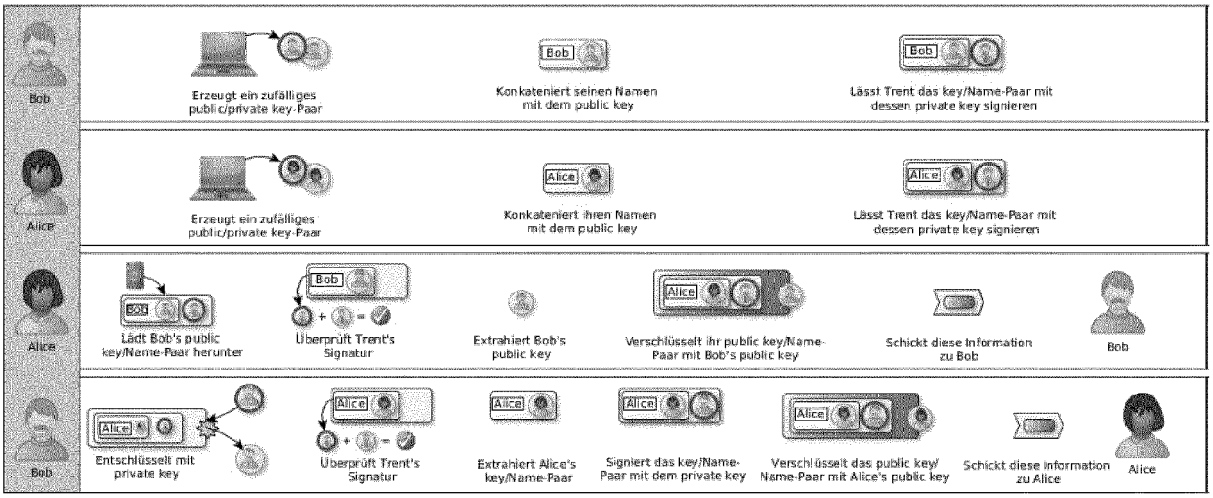
19. Verfahren nach Anspruch 15, ferner umfassend den Schritt:

- Verschlüsseln der ersten Dokumentenkennung (ID1) vor dem Versenden an den Nutzer.

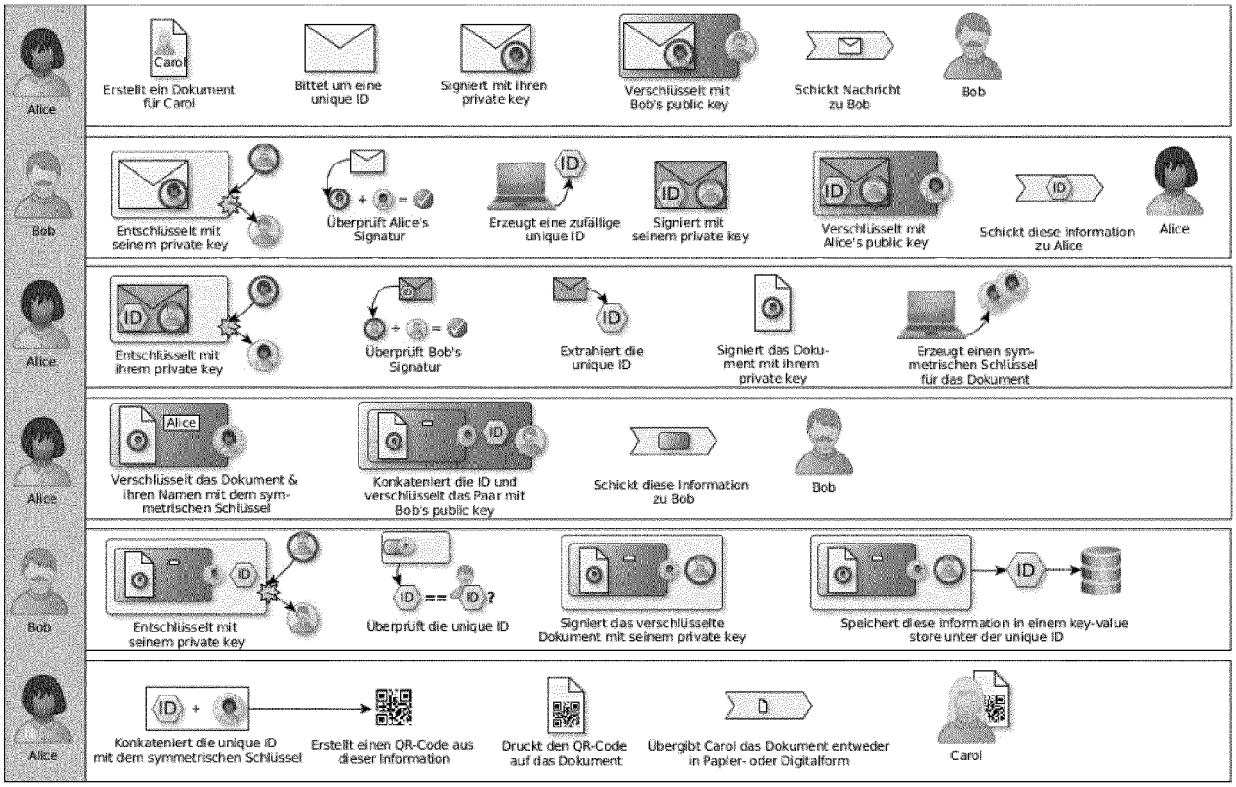
Figur 1

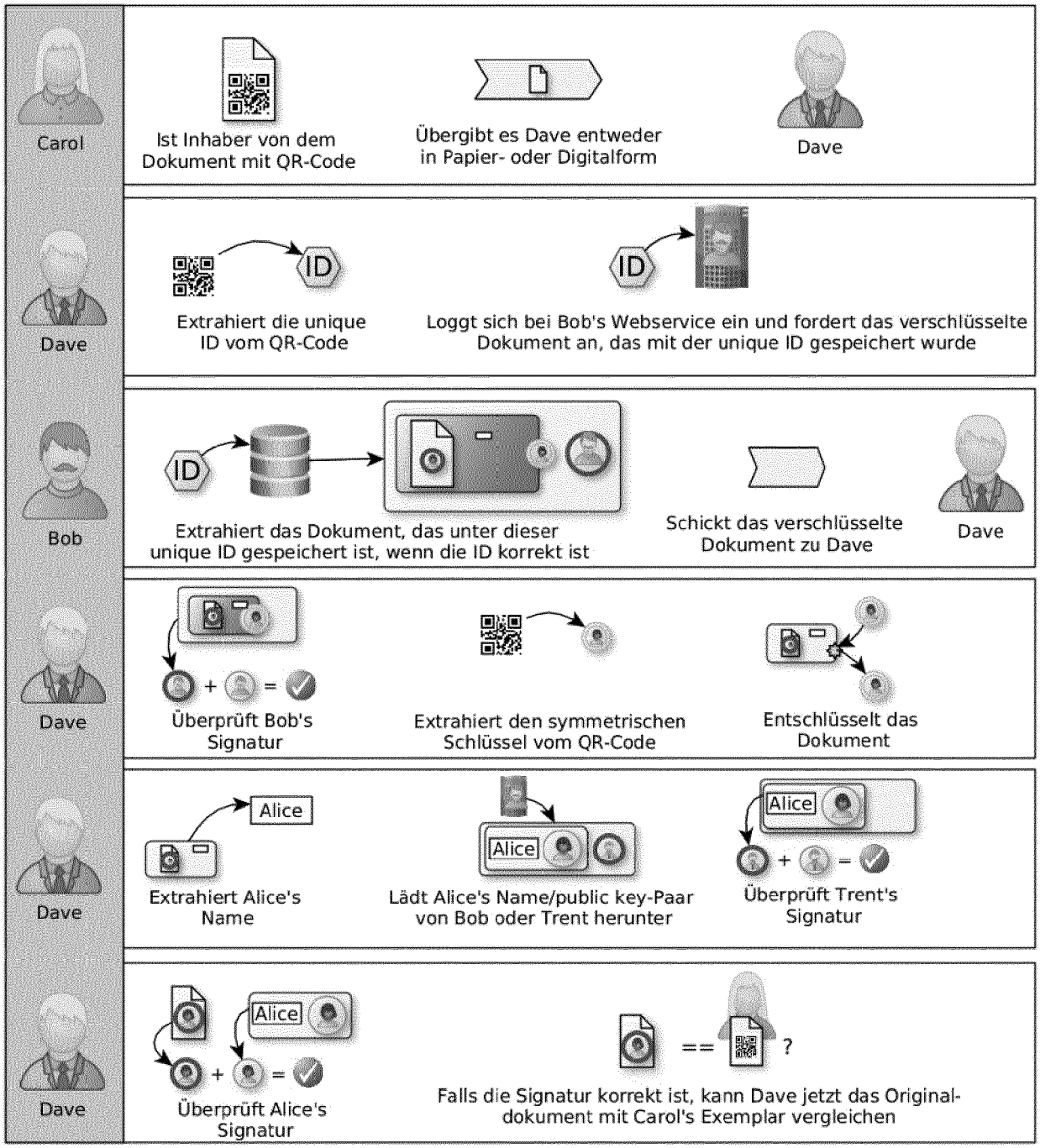

Bob
130
135
Certificate
Request
D2
Dave
120
Trent
Request
Certificate
dok_id
D2
110
115
D1
D1
Alice
Carol

Figur 2

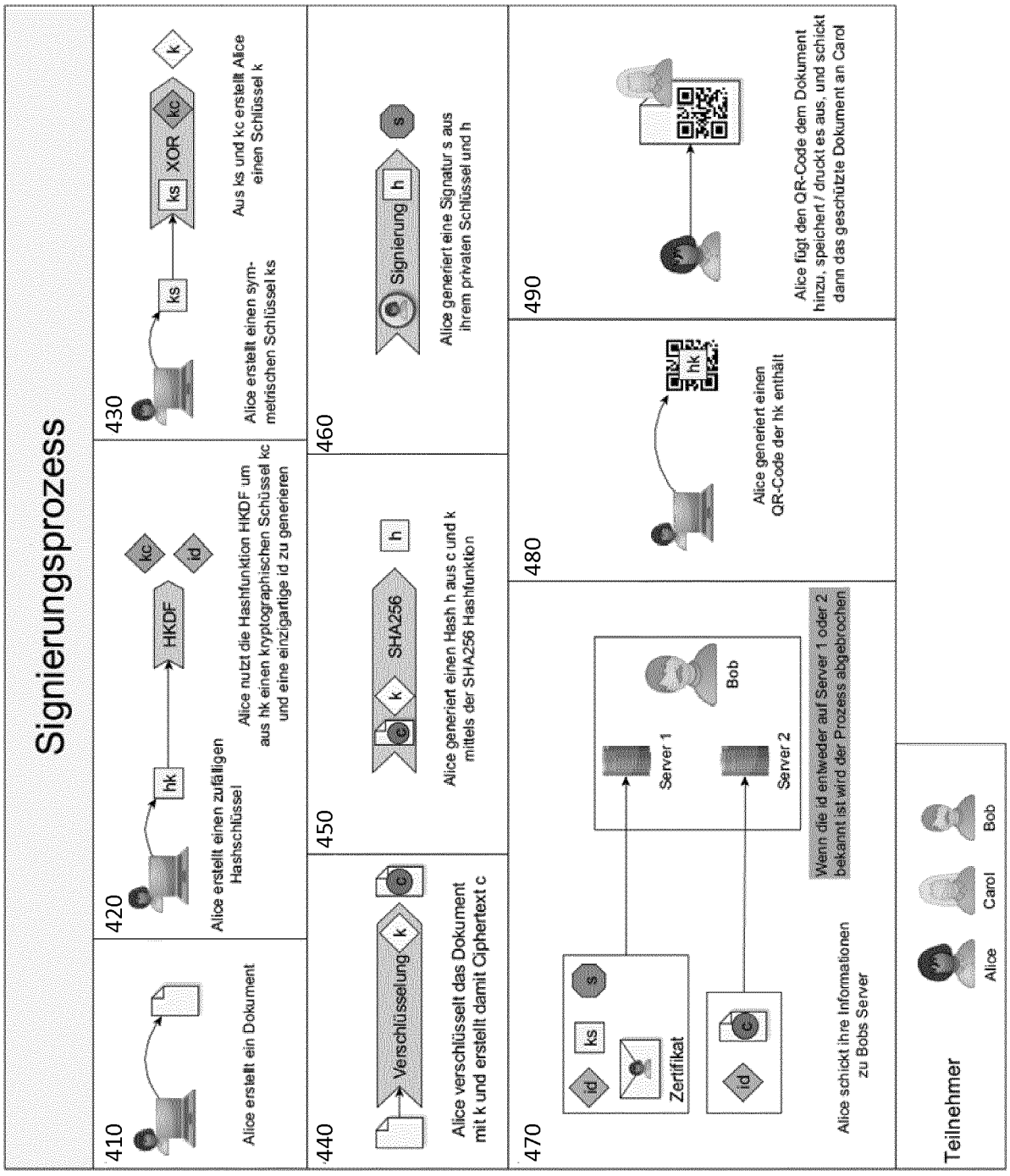


Figur 3

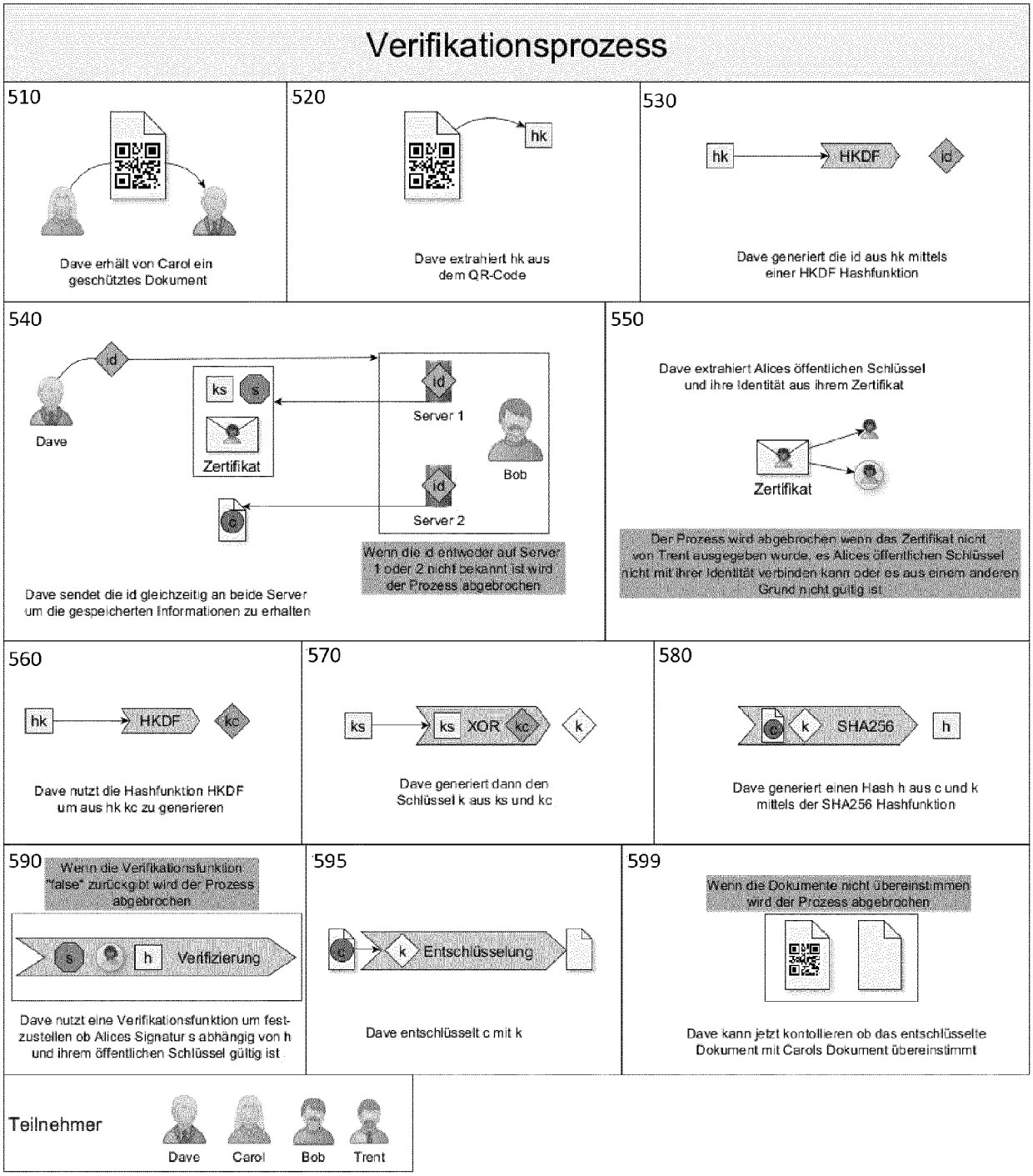



Carol
Ist Inhaber von dem Dokument mit QR-Code
Übergibt es Dave entweder in Papier- oder Digitalform
Dave
Dave
ID
Extrahiert die unique ID vom QR-Code
ID
Loggt sich bei Bob's Webservice ein und fordert das verschlüsselte Dokument an, das mit der unique ID gespeichert wurde
Bob
ID
Extrahiert das Dokument, das unter dieser unique ID gespeichert ist, wenn die ID korrekt ist
Schickt das verschlüsselte Dokument zu Dave
Dave
Dave
Überprüft Bob's Signatur
Extrahiert den symmetrischen Schlüssel vom QR-Code
Entschlüsselt das Dokument
Dave
Alice
Extrahiert Alice's Name
Alice
Lädt Alice's Name/public key-Paar von Bob oder Trent herunter
Alice
Überprüft Trent's Signatur
Dave
Alice
Überprüft Alice's Signatur
==
?
Falls die Signatur korrekt ist, kann Dave jetzt das Original-dokument mit Carol's Exemplar vergleichen

Figur 4


Signierungsprozess
410
Alice erstellt ein Dokument
420
hk
HKDF
kc
id
Alice erstellt einen zufälligen Hashschlüssel
Alice nutzt die Hashfunktion HKDF um aus hk einen kryptographischen Schlüssel kc und eine einzigartige id zu generieren
430
ks
XOR
kc
k
Alice erstellt einen symmetrischen Schlüssel ks
Aus ks und kc erstellt Alice einen Schlüssel k
440
Verschlüsselung
k
c
Alice verschlüsselt das Dokument mit k und erstellt damit Ciphertext c
450
c
k
SHA256
h
Alice generiert einen Hash h aus c und k mittels der SHA256 Hashfunktion
460
Signierung
h
s
Alice generiert eine Signatur s aus ihrem privaten Schlüssel und h
470
id
ks
s
Zertifikat
Server 1
Bob
Server 2
Alice schickt ihre Informationen zu Bobs Server
Wenn die id entweder auf Server 1 oder 2 bekannt ist wird der Prozess abgebrochen
480
hk
Alice generiert einen QR-Code der hk enthält
490
Alice fügt den QR-Code dem Dokument hinzu, speichert / druckt es aus, und schickt dann das geschützte Dokument an Carol
Teilnehmer
Alice
Carol
Bob

Figur 5


Verifikationsprozess
510
Dave erhält von Carol ein geschütztes Dokument
520
hk
Dave extrahiert hk aus dem QR-Code
530
hk
HKDF
id
Dave generiert die id aus hk mittels einer HKDF Hashfunktion
540
id
Dave
ks
s
Zertifikat
id
Server 1
Bob
id
Server 2
c
Wenn die id entweder auf Server 1 oder 2 nicht bekannt ist wird der Prozess abgebrochen
Dave sendet die id gleichzeitig an beide Server um die gespeicherten Informationen zu erhalten
550
Dave extrahiert Alices öffentlichen Schlüssel und ihre Identität aus ihrem Zertifikat
Zertifikat
Der Prozess wird abgebrochen wenn das Zertifikat nicht von Trent ausgegeben wurde, es Alices öffentlichen Schlüssel nicht mit ihrer Identität verbinden kann oder es aus einem anderen Grund nicht gültig ist
560
hk
HKDF
kc
Dave nutzt die Hashfunktion HKDF um aus hk kc zu generieren
570
ks
ks XOR kc
k
Dave generiert dann den Schlüssel k aus ks und kc
580
c
k
SHA256
h
Dave generiert einen Hash h aus c und k mittels der SHA256 Hashfunktion
590
Wenn die Verifikationsfunktion "false" zurückgibt wird der Prozess abgebrochen
s
h
Verifizierung
Dave nutzt eine Verifikationsfunktion um fest-zustellen ob Alices Signatur s abhängig von h und ihrem öffentlichen Schlüssel gültig ist
595
c
k
Entschlüsselung
Dave entschlüsselt c mit k
599
Wenn die Dokumente nicht übereinstimmen wird der Prozess abgebrochen
Dave kann jetzt kontollieren ob das entschlüsselte Dokument mit Carols Dokument übereinstimmt
Teilnehmer
Dave
Carol
Bob
Trent

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 17 18 7030

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	US 2005/138382 A1 (HOUGAARD TODD R [US] ET AL) 23. Juni 2005 (2005-06-23) * Zusammenfassung * * Absatz [0029] - Absatz [0031] * * Absatz [0035] - Absatz [0036] * * Absatz [0039] * * Absatz [0044] * * Absatz [0048] - Absatz [0049] * * Absatz [0055] - Absatz [0056] * * Abbildungen 1, 2, 3 * -----	1-19	INV. G06Q50/00
X	EP 0 850 523 A1 (DOCUMENT AUTHENTICATION SYSTEM [US]) 1. Juli 1998 (1998-07-01) * Zusammenfassung * * Spalte 4, Zeile 22 - Spalte 7, Zeile 22 * * Spalte 8, Zeile 63 - Spalte 10, Zeile 64 * * Abbildungen 1, 6a, 6b, 7, 8, 9 * -----	1-19	
X	US 2015/358163 A1 (CARTER PAUL L [NZ]) 10. Dezember 2015 (2015-12-10) * Zusammenfassung * * Absatz [0021] - Absatz [0022] * * Absatz [0024] - Absatz [0034] * * Absatz [0072] * * Abbildungen 1, 7 * -----	1-19	RECHERCHIERTE SACHGEBIETE (IPC) G06Q

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	2. November 2017	Stark, Konrad

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 17 18 7030

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

02-11-2017

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005138382 A1	23-06-2005	AU 2004308495 A1	14-07-2005
		CA 2594018 A1	14-07-2005
		EP 1703886 A2	27-09-2006
		US 2005138382 A1	23-06-2005
		WO 2005062968 A2	14-07-2005
EP 0850523 A1	01-07-1998	AU 714220 B2	23-12-1999
		BR 9610720 A	21-12-1999
		CA 2232170 A1	03-04-1997
		CN 1202288 A	16-12-1998
		CZ 9800787 A3	14-10-1998
		EP 0850523 A1	01-07-1998
		HK 1017540 A1	29-04-2005
		HU 9802232 A2	28-01-1999
		IL 123663 A	10-03-2002
		JP H11512841 A	02-11-1999
		KR 100455327 B1	31-12-2004
		KR 20040063988 A	15-07-2004
		NO 981170 A	13-05-1998
		NZ 318941 A	29-07-1999
		PL 326075 A1	17-08-1998
		TR 9800462 T1	22-06-1998
		US 5748738 A	05-05-1998
		WO 9712460 A1	03-04-1997
US 2015358163 A1	10-12-2015	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82