



SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 720 922 A1**

Patentanmeldung für die Schweiz und Liechtenstein

Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(51) Int. Cl.: **G06F 16/93** (2019.01)
G06F 16/31 (2019.01)
G06F 16/38 (2019.01)
G06F 21/62 (2013.01)
G06F 21/64 (2013.01)

(12) **PATENTANMELDUNG**

(21) Anmeldenummer: 000725/2023

(71) Anmelder:
KMS AG, Zumhofstrasse 10
6010 Kriens (CH)

(22) Anmeldedatum: 07.07.2023

(72) Erfinder:
Patrick Stücklin c/o KMS AG, 6010 Kriens (CH)
Marcel Steiner c/o KMS AG, 6010 Kriens (CH)
Armin Arnegger c/o KMS AG, 6010 Kriens (CH)

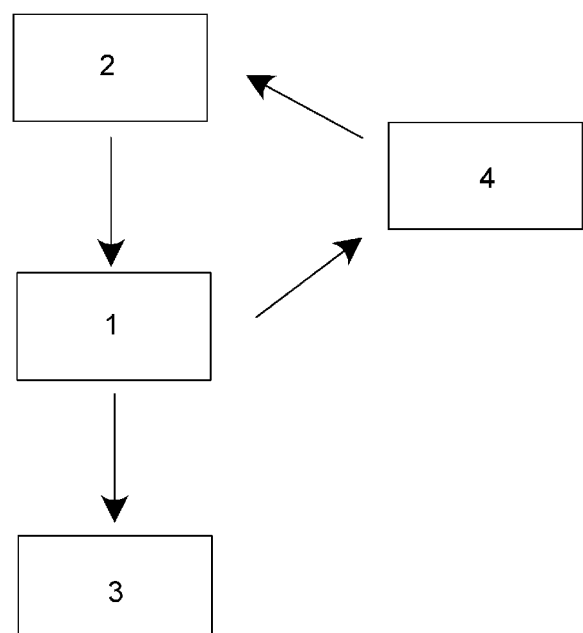
(43) Anmeldung veröffentlicht: 15.01.2025

(74) Vertreter:
IPrime Rentsch Kaelin AG, Hirschengraben 1
8001 Zürich (CH)

(54) **VERFAHREN UND SYSTEM ZUM DOKUMENTENUPLOAD**

(57) Die Erfindung betrifft ein Verfahren und System zum Erfassen, Hochladen und Verarbeiten von Dokumenten. Das Verfahren umfasst die folgenden Schritte: Anmelden eines Benutzers auf einem Endbenutzergerät (1), das mit einem Server (3) datentechnisch verbunden ist, Vornahme einer Dokumentattributisierung, Erfassen eines Dokuments, Signieren des erfassten Dokuments, Senden des erfassten signierten Dokuments an den Server (3), und Überprüfen des erfassten signierten Dokuments, wobei bei positiver Prüfung das Dokument zur Verarbeitung freigegeben wird.

Ferner betrifft die Erfindung ein mobiles Gerät und ein Computersystem.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Erfassen, Hochladen und Verarbeiten von Dokumenten. Weiterhin betrifft die vorliegende Erfindung ein mobiles Gerät zur Ausführung des Verfahrens sowie ein Computersystem.

Technologischer Hintergrund

[0002] Die Bereiche der Dokumentenerfassung, des Uploads und der Verarbeitung sind integrale Bestandteile des umfassenderen Bereichs der Dokumentenmanagementsysteme (DMS).

[0003] Die Dokumentenerfassung umfasst den Prozess der Erfassung, Digitalisierung und Konvertierung von Dokumenten in ein Format, das effektiv genutzt, verwaltet und gespeichert werden kann. Mit dem Aufkommen der OCR- (Optische Zeichenerkennung), ICR- (Intelligente Zeichenerkennung) und IDR-Technologien (Intelligente Dokumentenerkennung) hat dieser Bereich eine nie dagewesene Bedeutung erlangt. Sie ermöglichen es Computern, Text und Zeichen aus einer Vielzahl von Quellen zu erkennen, darunter gescannte Dokumente, Fotos und sogar Handschrift, was einen bedeutenden Sprung gegenüber den herkömmlichen manuellen Eingabemethoden darstellt. Nicht nur wird durch die Automatisierung des Prozesses Zeit und Ressourcen gespart, sondern die digitale Transformation der Dokumente verbessert auch die Genauigkeit und Verlässlichkeit der Daten. Darüber hinaus wird durch die Digitalisierung von Dokumenten der Zugang und die Suche nach Informationen erheblich erleichtert, was eine verbesserte Geschäftsprozesseffizienz und Produktivität zur Folge hat.

[0004] Der Upload-Prozess, der die Brücke zwischen Erfassung und Verarbeitung schlägt, umfasst die Übertragung der erfassten digitalen Dokumente an einen Server oder ein Cloud-basiertes Speichersystem. Dieser Prozess wurde durch Fortschritte in der Netzwerktechnologie, beim Cloud Computing und bei sicheren Verschlüsselungsmethoden revolutioniert. Es ist jetzt möglich, grosse Mengen von Dokumenten schnell und sicher hochzuladen, wodurch Unternehmen Zeit und Ressourcen sparen und gleichzeitig die Risiken von Datenschutzverletzungen verringern können.

[0005] Gleichzeitig ermöglicht die Verwendung fortschrittlicher Verschlüsselungsmethoden während des Upload-Prozesses eine höhere Sicherheitsstufe. Dadurch können Unternehmen das Risiko von Datenverlusten oder -verletzungen minimieren, die möglicherweise zu erheblichen finanziellen Verlusten oder rechtlichen Konsequenzen führen könnten. Die moderne Verschlüsselungstechnologie bietet nicht nur die Möglichkeit, Dokumente während der Übertragung zu schützen, sondern auch sicherzustellen, dass die Dokumente in der Cloud sicher gespeichert sind.

[0006] Zusätzlich zur bereits erwähnten Verschlüsselungstechnologie haben Zertifikate und digital signierte Dokumente einen wichtigen Platz im modernen Upload-Prozess eingenommen, um Sicherheit und Authentizität zu gewährleisten. Digitale Zertifikate sind eine Art von „digitaler Ausweis“, der dazu dient, die Identität eines Benutzers oder eines Systems während des Datenübertragungsprozesses zu überprüfen. Sie werden von einer vertrauenswürdigen dritten Partei, einer sogenannten Zertifizierungsstelle ausgestellt und können verwendet werden, um zu bestätigen, dass die Daten von der angegebenen Quelle stammen und dass sie während der Übertragung nicht manipuliert wurden. In diesem Sinne tragen sie dazu bei, die Integrität der übertragenen Daten sicherzustellen und das Vertrauen in den Upload-Prozess zu stärken.

[0007] In der letzten Phase, der Dokumentenverarbeitung, werden die hochgeladenen Dokumente kategorisiert, indiziert und für einen einfachen Abruf gespeichert. Hier kommen Computer Vision und maschinelles Lernen zum Einsatz, um die automatische Extraktion relevanter Daten und Metadaten, die semantische Analyse und die intelligente Klassifizierung von Dokumenten durchzuführen. Darüber hinaus hat die Verarbeitung natürlicher Sprache Funktionen wie Stimmanalyse und automatische Zusammenfassungen eingeführt, die es Unternehmen ermöglichen, aussagekräftige Erkenntnisse aus ihren Dokumenten abzuleiten.

[0008] Doch so vielversprechend diese Fortschritte auch sein mögen, es bleiben Herausforderungen bestehen. Aufgrund des sensiblen Charakters einiger Dokumente stehen Datenschutz- und Sicherheitsbedenken weiterhin an erster Stelle. Auch Interoperabilitätsprobleme können aufgrund der unterschiedlichen Dokumentenformate und -systeme auftreten. Ausserdem ist es trotz der Leistungsfähigkeit moderner OCR- und NLP-Techniken nach wie vor eine Herausforderung, komplexe Layouts oder handgeschriebenen Text genau zu erkennen und zu verarbeiten.

[0009] Aus dem Stand der Technik ist CH714700B1 bekannt. Es offenbart ein computerimplementiertes Verfahren und System zur effizienten Erfassung von Personendaten und zugehörigen Dokumenten. Es beinhaltet die Verknüpfung eines Datenobjekts und eines Personenidentifikators innerhalb eines Computersystems. Es wird ein visueller Code erzeugt, der Referenzinformationen zur Identifizierung des verknüpften Datenobjekts kodiert. Es wird eine visuelle Darstellung des Codes erstellt. Die im visuellen Code kodierten Referenzinformationen werden in einem mobilen Kommunikationsgerät mit dessen Kamera erfasst und gespeichert. Anschliessend wird in dem mobilen Kommunikationsgerät ein Datenpaket erzeugt, das die erfassten Referenzinformationen und ein Bild eines zu der Person gehörenden Dokuments enthält. Dieses Datenpaket wird dann an das Computersystem übermittelt. Nach dem Empfang des Pakets speichert das Computersystem das Bild des Dokuments und verknüpft es auf der Grundlage der Referenzinformationen mit dem Datenobjekt.

[0010] Darüber hinaus stellt US2013083362 ein Informationsverarbeitungsgerät vor, das effizient in der Dateibearbeitung und -speicherung ist. Das Gerät besteht aus einem ersten Steuergerät, das eine Datei erfasst, sowie einem zweiten Steuergerät, das Bereichsinformationen empfängt, die den Speicherplatz der Datei auf einem spezifischen Speichermedium angeben. Zudem ist das Gerät mit einem Generator-Controller ausgestattet, der eine zweite Datei aus der ursprünglichen

erzeugt und einen zusätzlichen Abschnitt zur Aufnahme von weiteren Daten einfügt. Die Bereichsinformationen vom zweiten Steuergerät werden durch die Aktivitäten eines Speichercontrollers als zusätzliche Daten in der neuen Datei gesichert. Diese Bereichsinformationen können als codierte Daten kodiert, in einem Thumbnail-Bereich als verkleinertes Bild gespeichert oder sogar für die Dateiübertragung mit externen Speichergeräten kommuniziert werden. Interessanterweise kann die zweite Datei in demselben oder einem anderen Format als die erste Datei erzeugt werden, wobei Formate wie JPEG, PDF und TIFF unterstützt werden. Sowohl eine Reduzierung des Datenbestands in der zweiten Datei als auch die Erfassung von Bilddaten zur Erstellung der ersten Datei sind ebenfalls möglich. Darüber hinaus umfasst die Veröffentlichung nicht nur das Gerät selbst, sondern auch ein nicht übertragbares, computerlesbares Speichermedium, das ein Informationsverarbeitungsprogramm zur Ausführung dieser Funktionen beinhaltet, sowie ein Verfahren zur Durchführung des Dateiverarbeitungsprozesses.

[0011] US2016253161 betrifft ein Informationsverarbeitungsgerät, das mit zwei Servern und einem externen Gerät interagiert. Das Gerät erhält Zugangsinformationen und andere Informationen von einem Zielobjekt und sendet diese an den ersten Server. Im Gegenzug liefert der Server eindeutige Identifikations- und Zugangsinformationen für den zweiten Server. Diese Informationen werden auf dem Gerät gespeichert, das dann den Zugriff auf den zweiten Server anfordert, um ein Anwendungsprogramm herunterzuladen und zu installieren. Sobald die Anwendung installiert ist, kann das Gerät Anweisungen zu ihrer Aktivierung entgegennehmen. Die gespeicherten Identifizierungsinformationen werden an den ersten Server zurückgesendet, um eindeutige Informationen zu dieser Identifizierung zu erhalten. Dadurch kann das Anwendungsprogramm eine Verbindung mit einem externen Gerät herstellen und eine Kommunikationsverarbeitung durchführen. Die Erfindung umfasst ferner ein Browserprogramm, eine Bildverarbeitung, eine drahtlose Nahfeldkommunikation, ein Codeschema-Lesegerät, Gerätesteuerverfahren und ein Kommunikationssystem.

[0012] US2017094101 beschreibt ein Managementsystem, das die Kommunikation zwischen einem Bildverarbeitungsgerät, einem Endgerät und dem System selbst erleichtert. Es umfasst eine Netzwerkschnittstelle und einen Controller. Der Controller empfängt Positionsinformationsanforderungen von der Bildverarbeitungsvorrichtung, überträgt Originalbildpositionsinformationen, speichert die Originalbilddaten und sendet Codedaten, um Zielbildpositionsinformationen zu erfassen. Anschliessend empfängt das System Zielbilddatenanforderungen vom Endgerät und überträgt die entsprechenden Daten. Weitere Funktionen sind die Erzeugung von Positionsinformationen, das Löschen von Daten, die Handhabung verschiedener Netzwerkschnittstellen, die Konvertierung von Bilddaten und die Anzeige von interaktiven Seitendaten. Die Erfindung umfasst auch ein Kommunikationssystem und ein computerlesbares Speichermedium mit Programmanweisungen.

Darstellung der Erfindung

[0013] Eine Aufgabe der Erfindung besteht darin mindestens einige der Nachteile des Standes der Technik zu vermeiden.

[0014] Diese Aufgabe wird durch die Merkmale der unabhängigen Patentansprüche gelöst.

[0015] Die erfindungsgemässe Lösung weist ein Verfahren zum Erfassen, Hochladen und Verarbeiten von Dokumenten auf. Das Verfahren umfasst die folgenden Schritte: Anmelden eines Benutzers auf einem Endbenutzergerät, das mit einem Server datentechnisch verbunden ist, Erfassen eines Dokuments, Vornahme einer Dokumentattributisierung, Signieren des erfassten Dokuments, Senden des erfassten signierten Dokuments an den Server, und Überprüfen des erfassten signierten Dokuments, wobei bei positiver Prüfung das Dokument zur Verarbeitung freigegeben wird.

[0016] Die Vornahme der Dokumentattributisierung oder Attributisierung kann durch ein Bereitstellen einer oder mehrerer Auswahllisten erfolgen. Dabei kann ein Mandant, Jahr, Kanton oder beispielsweise eine Kategorie wie Lohnausweis, Jahresrechnung, Saldobilanz, Kontoblätter, Vertrag u.ä. angegeben werden, um eine entsprechende Zuordnung zu erleichtern. Die Dokumentattributisierung kann sequenziell oder zeitlich unabhängig erfolgen.

[0017] Ergänzend kann dieses Verfahren die Integration von künstlicher Intelligenz vorsehen. Diese kann zur Verbesserung des Dokumentenerfassungs- und Überprüfungsprozesses beitragen, indem sie beispielsweise automatische Texterkennung (OCR) oder maschinelles Lernen für die Dokumentklassifikation einsetzt. Diese Technologien könnten die Genauigkeit und Geschwindigkeit der Dokumentverarbeitung erheblich steigern.

[0018] Die erfindungsgemässe Lösung kann durch die folgenden weiteren, jeweils für sich vorteilhaften Ausführungen ergänzt und weiter verbessert werden.

[0019] Gemäss einer Ausführungsform ist vorgesehen, dass das Verfahren weiter eine Kategorisierung des Dokuments, des erfassten Dokuments und/oder des erfassten signierten Dokuments auf der Grundlage der Dokumentattributisierung umfasst.

[0020] Die Einbeziehung der Kategorisierung des Dokuments, des erfassten Dokuments und/oder des erfassten signierten Dokuments in das Verfahren bietet eine Reihe von Vorteilen.

[0021] Erstens ermöglicht diese Kategorisierung eine verbesserte Organisation von Dokumenten. Es erleichtert Benutzern das Auffinden von spezifischen Dokumenten aus einer Vielzahl von Dateien und reduziert die benötigte Zeit, um auf diese Dokumente zuzugreifen.

[0022] Zweitens erhöht die Kategorisierung die Effizienz der Dokumentenverarbeitung. Durch die Gruppierung ähnlicher Dokumente zusammen auf der Grundlage ihrer Dokumentattribute können bestimmte Verarbeitungsaufgaben, wie zum

Beispiel die Extraktion bestimmter Informationen oder die Durchführung spezifischer Analysen, leichter und schneller durchgeführt werden.

[0023] Drittens könnte die Kategorisierung zur Verbesserung der Datenanalyse und des Berichtswesens beitragen. Mit den kategorisierten Dokumenten können Benutzer Trends und Muster innerhalb bestimmter Kategorien von Dokumenten besser erkennen.

[0024] Ergänzend kann maschinelles Lernen und künstliche Intelligenz in die Dokumentattributisierung integriert werden, um beispielsweise die Dokumentklassifizierung in einer fortschrittlichen Systematik vorzunehmen. Diese Systematik erleichtert die eindeutige Zuweisung von Dokumenten und ermöglicht eine thematische Gruppierung und Priorisierung.

[0025] Zum Beispiel kann ein Dokument, das als vertraulich markiert ist, aufgrund seines Dokumentattributs automatisch in einem sicheren Speicherbereich gespeichert werden. Dokumente, die sich auf ein spezifisches Projekt beziehen, könnten automatisch dem entsprechenden Projektordner zugewiesen werden. Dies vereinfacht erheblich die Organisation und den Zugriff auf relevante Informationen.

[0026] Des Weiteren könnte ein Algorithmus entwickelt werden, der den Inhalt eines erfassten Dokuments analysiert und automatisch eine Reihe relevanter Dokumentattribute zuweist. Diese könnten Aspekte wie das Dokumententhema, die beteiligten Personen oder Unternehmen, die Art des Dokuments (z. B. Rechnung, Vertrag, technische Spezifikation) und den Zeithorizont umfassen.

[0027] Darüber hinaus könnten Dokumentattribute dazu genutzt werden, den Dokumentenstatus zu kennzeichnen, etwa ob es sich um eine Entwurfs- oder eine endgültige Version handelt, ob das Dokument genehmigt wurde oder noch eine Genehmigung erfordert. Dies würde eine effizientere und transparentere Dokumentenverwaltung ermöglichen.

[0028] Zusätzlich bietet die Dokumentattributisierung die Möglichkeit, eine effizientere Suchfunktion zu implementieren, die nicht nur nach Dokumenttiteln, sondern nach allen Dokumentattributen suchen könnte. Dies könnte die Effizienz bei der Dokumentensuche deutlich steigern, insbesondere in umfangreichen oder komplexen Dokumentenarchiven.

[0029] Schliesslich könnte ein solches System auch Benachrichtigungen senden, wenn Dokumente erstellt, geändert oder genehmigt werden, basierend auf den ihnen zugewiesenen Dokumentattributen. Dies würde die Zusammenarbeit und Kommunikation innerhalb von Teams und Abteilungen verbessern.

[0030] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Erfassen eines Dokuments eine Bildbearbeitung, insbesondere eine Perspektivenkorrektur und/oder eine Kontrastoptimierung und/oder eine Datenextraktion umfasst.

[0031] Dadurch kann eine Verbesserung des erfassten Dokuments erreicht werden, um eine optimale Weiterverarbeitung zu ermöglichen. Eine Datenextraktion erlaubt eine genauere Zuordnung und Abspeicherung z.B. in einer Datenbank. Vorteilhafterweise können Daten durch Automatisierung oder Verifizierung in vorgesehene Felder eingefügt oder hinzugefügt werden, z.B. durch unterschiedliche Farben, was die Unterscheidung der Daten vereinfacht. Felder können mit einer Datenherkunft versehen werden, was für die Nachbearbeitung hilfreich sein kann. Ein Fehler-Assistent kann die extrahierten Daten überprüfen und bei Unstimmigkeiten markieren.

[0032] Darüber hinaus könnten Benutzerprofile erstellt werden, um den Prozess des Erfassens und Verarbeitens der Dokumente auf individuelle Benutzeranforderungen zuzuschneiden. Beispielsweise könnten persönliche Präferenzen bezüglich Kontrastoptimierung oder Perspektivenkorrektur berücksichtigt werden.

[0033] Für die Datenüberprüfung könnte zusätzlich zu einem Fehler-Assistenten ein Echtzeit-Feedback-System implementiert werden, das Unstimmigkeiten sofort erkennt und den Benutzer darauf aufmerksam macht. Das Feedback-System könnte auch Vorschläge zur Behebung der Unstimmigkeiten liefern, um den Prozess der Nachbearbeitung zu optimieren.

[0034] Es könnte ebenfalls ein System zur Datenvalidierung eingeführt werden, das sicherstellt, dass die extrahierten Daten korrekt und vollständig sind. Ein solches System könnte auf Algorithmen basieren, welche die Daten auf Konsistenz und Plausibilität überprüfen und bei Bedarf eine automatische Korrektur vornehmen.

[0035] Das Anmelden eines Benutzers kann durch ein biometrisches Login erfolgen, was eine benutzerfreundliche und identitätsgeprüfte Anmeldung ermöglicht. Biometrische Daten sind einzigartig für jeden Einzelnen und umfassen Merkmale wie Fingerabdrücke, Iris-Muster, Stimmuster, Gesichtsstruktur und sogar Verhaltensmuster wie Tippgeschwindigkeit oder Bewegungsabläufe.

[0036] Wenn ein Benutzer sich in ein System einloggen möchte, könnte dieser aufgefordert werden, ein biometrisches Merkmal bereitzustellen, beispielsweise einen Fingerabdruck oder eine Gesichtserkennung. Ein spezialisierter Scanner würde dann dieses Merkmal abtasten oder aufnehmen und die gewonnenen Daten mit einer zuvor gespeicherten Referenz dieses Merkmals vergleichen. Falls die erfassten Daten und die gespeicherte Referenz übereinstimmen, wird der Benutzer erfolgreich authentifiziert und erhält Zugang zum System.

[0037] Um die Sicherheit weiter zu erhöhen, könnte eine Mehrfaktor-Authentifizierung implementiert werden. Bei dieser Methode muss der Benutzer zusätzlich zur biometrischen Authentifizierung noch einen weiteren Authentifizierungsfaktor bereitstellen, wie zum Beispiel ein Passwort, biometrische Daten oder einen per SMS gesendeten Code.

[0038] Die Verwendung von biometrischen Daten zur Authentifizierung bietet ein hohes Mass an Sicherheit, da biometrische Merkmale schwer zu fälschen oder zu stehlen sind. Gleichzeitig kann es für den Benutzer sehr bequem sein, da er sich keine komplizierten Passwörter merken muss.

[0039] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass die Vornahme der Dokumentattributisierung in Erwiderung auf das Anmelden erfolgt.

[0040] Indem die Dokumentattributisierung direkt nach dem Anmelden erfolgen kann, wird eine nahtlose und schnelle Bearbeitung des Dokuments ermöglicht. Dies kann dazu beitragen, Verzögerungen im Workflow zu minimieren und gleichzeitig die Benutzerfreundlichkeit zu erhöhen.

[0041] Darüber hinaus erhöht die frühe Dokumentattributisierung die Genauigkeit und Relevanz der erfassten Daten. Sie erlaubt es, relevante Informationen über das Dokument und dessen Kontext zu sammeln, wodurch eine genauere Kategorisierung und Verarbeitung des Dokuments ermöglicht werden. Je genauer und relevanter die Daten sind, desto höher ist die Qualität der nachfolgenden Prozesse, wie z.B. die Datenextraktion oder die Bildbearbeitung.

[0042] Ein weiterer Vorteil dieses Ansatzes besteht darin, dass er eine Personalisierung des Prozesses ermöglicht. Indem die Dokumentattributisierung basierend auf dem angemeldeten Benutzer vorgenommen wird, kann das System den Prozess auf die individuellen Bedürfnisse und Präferenzen des Benutzers abstimmen. Dies kann beispielsweise dazu genutzt werden, um die Liste der Dokumente nach Dokumentattributen, z.B. Mandanten und/oder Steuerjahr, zu gruppieren und weitere Filter und Gruppierungsmöglichkeiten anzubieten.

[0043] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Verfahren ferner ein Abfragen von auf dem Server gespeicherten Dokumenten umfasst.

[0044] Dies bietet ein umfassendes Bild oder eine Übersicht über bereits hochgeladene Dokumente für das Endbenutzergerät und hilft somit, Doppelspurigkeiten zu vermeiden.

[0045] Ferner, durch das Abfragen von auf dem Server gespeicherten Dokumenten, können Benutzer schnell und einfach auf ihre Dokumente zugreifen, ohne zusätzliche Anforderungen oder Tools zu benötigen. Dies spart Zeit und vereinfacht den Prozess, insbesondere für Benutzer, die regelmässig auf bestimmte Dokumente zugreifen müssen.

[0046] Diese Funktion verbessert auch die Effizienz des Systems. Anstatt Dokumente erneut hochladen oder bearbeiten zu müssen, können Benutzer einfach auf bestehende Dokumente zugreifen. Das bedeutet, dass weniger Datenverkehr generiert wird und der Server effizienter arbeiten kann. Ausserdem könnte diese Funktion auch die Leistung des Systems verbessern, indem sie redundante Prozesse minimiert und somit Ressourcen einspart.

[0047] Darüber hinaus ermöglicht diese Funktion eine bessere Dokumentenverwaltung. Mit der Fähigkeit, auf dem Server gespeicherte Dokumente abzufragen, können Benutzer ihre Dokumente leichter organisieren und verwalten. Sie könnten beispielsweise bestimmte Dokumente für eine spätere Verwendung markieren oder Dokumente nach verschiedenen Kriterien filtern, wie z.B. Erstellungsdatum, Autor oder Dateityp.

[0048] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Dokument und/oder erfasste Dokument, und/oder erfasste signierte Dokument auf dem Endbenutzergerät flüchtig gespeichert werden/wird.

[0049] Mit „flüchtig“ ist in der Regel gemeint, dass die Daten nur vorübergehend und oft nur für die Dauer einer Sitzung gespeichert werden, ähnlich dem Konzept von Cache-Speicher oder temporären Dateien in der Computertechnologie.

[0050] Erstens kann mit diesem Merkmal sichergestellt werden, dass die Dokumente für Unbefugte nicht mehr zugänglich sind, wenn beispielsweise das Endbenutzergerät ein mobiles Gerät ist, welches verloren gegangen ist.

[0051] Zunächst erhöht diese Methode die Sicherheit des Systems. Indem die Dokumente flüchtig gespeichert werden, wird das Risiko minimiert, dass sie im Falle eines Geräteverlusts oder -diebstahls abgerufen oder missbraucht werden können. Sobald der Benutzer seine Sitzung beendet oder das Gerät neu startet, werden die flüchtig gespeicherten Daten in der Regel gelöscht, was das Risiko einer dauerhaften Kompromittierung der Daten erheblich reduziert.

[0052] Zweitens kann dieses Merkmal die Leistung des Endbenutzergeräts verbessern. Da die Daten nur vorübergehend gespeichert werden, wird weniger Speicherplatz auf dem Gerät beansprucht. Dies kann dazu beitragen, dass das Gerät schneller und effizienter arbeitet, insbesondere bei Geräten mit begrenztem Speicherplatz.

[0053] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass nach dem Senden des erfassten signierten Dokuments an den Server das Dokument und/oder erfasste Dokument, und/oder erfasste signierte Dokument auf dem Endbenutzergerät nach positiver Prüfung ganz oder teilweise gelöscht werden/wird.

[0054] Damit kann sichergestellt werden, dass nur überprüfte und gültige Dokumente gelöscht werden. Eine Teillöschung kann bei grösseren Dokumenten in Betracht gezogen werden, sodass eine Speicheroptimierung stattfindet. Dies kann dazu beitragen, die Leistung des Geräts zu optimieren und sicherzustellen, dass es effizient funktioniert, insbesondere wenn der Speicherplatz erheblich begrenzt ist.

[0055] Darüber hinaus wird durch das Löschen der Daten auf dem Endbenutzergerät nach erfolgreicher Überprüfung und Übertragung an den Server das Risiko minimiert, dass sensible Informationen in falsche Hände geraten, weil die sensiblen Daten nicht mehr auf dem Gerät vorhanden sind.

[0056] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Verfahren ferner Aktualisieren einer Liste der an den Server gesendeten Dokumenten auf dem Endbenutzergerät umfasst.

[0057] Mit einer aktualisierten Liste der gesendeten Dokumente kann der Benutzer jederzeit den Überblick behalten, welche Dokumente bereits an den Server gesendet wurden. Dies kann dazu beitragen, Verwirrungen zu vermeiden und das Vertrauen des Benutzers in das System zu stärken.

[0058] Ferner verbessert dieses Merkmal die Benutzerfreundlichkeit des Systems. Die Benutzer haben dadurch einen einfachen und schnellen Zugang zu einer Übersicht aller gesendeten Dokumente, was den Such- und Zugriffsprozess erheblich vereinfacht. Sie könnten beispielsweise die Liste nach verschiedenen Kriterien durchsuchen oder filtern, um bestimmte Dokumente schneller zu finden.

[0059] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Dokument und/oder erfasste Dokument, und/oder erfasste signierte Dokument Metadaten enthalten kann.

[0060] Metadaten können eine Vielzahl von Informationen beinhalten, wie z.B. das Erstellungsdatum des Dokuments, den Erstellungsort, den Autor die Dokumentenart oder andere spezifische Merkmale. Dadurch kann der Benutzer oder das System schnell relevante Informationen über das Dokument erhalten, ohne das Dokument selbst öffnen und lesen zu müssen.

[0061] Zweitens kann das Einbeziehen von Metadaten die Effizienz des Systems steigern. Durch die Verwendung von Metadaten können Dokumente leichter kategorisiert, organisiert und abgerufen werden. Dies kann die Suche nach Dokumenten und die allgemeine Dokumentenverwaltung erheblich erleichtern.

[0062] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass nach positiver Prüfung des erfassten signierten Dokuments, das erfasste signierte Dokument, und/oder die Dokumentattributisierung, und/oder die zugehörigen Metadaten auf dem Server gespeichert werden.

[0063] Dies bietet mehrere Vorteile. Erstens erhöht eine separate oder externe Komponente für das Signieren der Dokumente die Sicherheit des Verfahrens. Da die Signaturfunktion von der Hauptanwendung isoliert ist, reduziert dies das Risiko einer umfassenden Systemkompromittierung. Falls ein Angreifer Zugang zum Hauptsystem erlangt, würde diese Trennung der Komponenten die Signaturfunktion und die damit verbundenen sensiblen Daten vor direktem Zugriff schützen.

[0064] Zweitens bietet diese Methode eine verbesserte Skalierbarkeit. Mit einer separaten Komponente zur Signierung der Dokumente kann das System leichter erweitert werden, um grössere Arbeitslasten zu bewältigen, ohne dass die Hauptanwendung beeinträchtigt wird. Wenn beispielsweise die Menge der zu signierenden Dokumente steigt, kann die Signaturkomponente entsprechend skaliert werden, um die höhere Arbeitslast zu bewältigen.

[0065] Drittens bringt eine separate oder externe Komponente für das Signieren der Dokumente Flexibilität in das System. Je nach den spezifischen Anforderungen und Umständen können verschiedene externe Signaturdienste oder -technologien eingesetzt werden, ohne dass die Hauptanwendung wesentlich geändert werden muss. Dies kann die Anpassung an verschiedene gesetzliche Anforderungen oder technologische Standards erleichtern.

[0066] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass das Verfahren ferner Signaturspeicherung des erfassten signierten Dokuments auf dem Endbenutzergerät und/oder Server umfasst.

[0067] Erstens, indem das signierte Dokument sowie die zugehörigen Metadaten und Kategorisierungen auf dem Server gespeichert werden, werden sie vor lokalen Bedrohungen auf dem Endbenutzergerät geschützt. Server sind in der Regel besser vor Datenverlust durch Hardware-Ausfälle geschützt und können so die Integrität und Verfügbarkeit der Daten sicherstellen.

[0068] Zweitens erleichtert die Speicherung von Dokumenten zusammen mit ihren Kategorisierungen und Metadaten die Datenverwaltung erheblich. Nutzer und Systemadministratoren können schnell und effizient auf benötigte Informationen zugreifen, sie filtern und sortieren, was den Arbeitsfluss beschleunigt und die Benutzererfahrung verbessert.

[0069] Ferner wird die Sicherheit des Systems durch die Speicherung der Signatur sowohl lokal auf dem Endbenutzergerät als auch auf dem Server erheblich erhöht, weil es erlaubt Manipulationen durch Dritte zu erkennen. In diesem Fall unterscheidet sich die Signatur zwischen dem Server und Endbenutzergerät und ein Dokument kann als ungültig und somit inkonsistent erklärt werden.

[0070] Darüber hinaus ist vorgesehen, eine Signaturkopie auf dem Endbenutzergerät zu speichern, damit die Nachvollziehbarkeit der erfassten signierten Dokumente auf dem Endbenutzergerät möglich ist.

[0071] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass die Prüfung des erfassten signierten Dokuments eine Konsistenz- und/oder Integritätsprüfung umfasst.

[0072] Die Datenintegrität wird durch diese Prüfungsmethode deutlich verbessert. Eine Konsistenzprüfung kann dazu dienen, sicherzustellen, dass das Dokument keine Widersprüche oder Inkonsistenzen enthält, welche die Gültigkeit oder Verständlichkeit des Dokuments beeinträchtigen könnten. Eine Integritätsprüfung hingegen stellt sicher, dass das Dokument seit seiner Erstellung oder letzten gültigen Änderung nicht verändert wurde. Zusammen können diese beiden Prüfungen dazu beitragen, dass die Daten in den erfassten Dokumenten korrekt, kohärent und vertrauenswürdig sind.

[0073] Die Verbesserung der Fehlererkennung ist ein weiterer Vorteil dieser Prüfungsmethode. Während der Konsistenz- und Integritätsprüfung können auch andere potenzielle Fehler oder Probleme im Dokument erkannt und markiert werden, was den Benutzern hilft, diese zu korrigieren und die Qualität der erfassten Dokumente zu verbessern.

[0074] Schliesslich stärkt diese Art der Prüfung das Vertrauen in die Gültigkeit der Dokumente. Durch die Bestätigung der Konsistenz und Integrität der Dokumente können Benutzer sicher sein, dass die Informationen, die sie betrachten oder verwenden, korrekt und unverändert sind. Dies kann für eine Vielzahl von Anwendungen von entscheidender Bedeutung sein, von der Verwaltung persönlicher Informationen bis hin zur Erfüllung rechtlicher Anforderungen.

[0075] Gemäss einer weiteren Ausführungsform ist vorgesehen, dass die Prüfung des erfassten signierten Dokuments auf dem Server erfolgt.

[0076] Zunächst einmal ermöglicht die serverseitige Prüfung eine bessere Leistung und weniger Belastung für das Endbenutzergerät. Server verfügen in der Regel über erheblich mehr Rechenleistung und Ressourcen als Endbenutzergeräte, wodurch sie in der Lage sind, komplexe Prüfungen und Berechnungen effizienter durchzuführen. Dies spart Zeit und Akkuleistung auf dem Endbenutzergerät und ermöglicht eine schnellere und flüssigere Benutzererfahrung.

[0077] Darüber hinaus ermöglicht die Durchführung der Prüfung auf dem Server eine verbesserte Skalierbarkeit. Da der Server die Prüfungen durchführt, kann das System leicht auf eine grosse Anzahl von Benutzern und Dokumenten skaliert werden, ohne die Leistung oder Funktionalität des einzelnen Endbenutzergeräts zu beeinträchtigen. Dies ist besonders wichtig für grosse Organisationen oder Systeme mit vielen Benutzern.

[0078] Schliesslich bietet die serverseitige Prüfung auch verbesserte Sicherheitsmerkmale. Da der Server die Kontrolle über die Prüfung hat, kann er sicherstellen, dass die Prüfungsprozesse und -ergebnisse vor Manipulationen geschützt sind. Darüber hinaus kann der Server auch bessere Protokollierungs- und Überwachungsfunktionen bieten, um verdächtige Aktivitäten zu erkennen und auf Sicherheitsprobleme zu reagieren.

[0079] Die erfindungsgemässe Lösung weist auch ein mobiles Gerät auf, dass Mittel zur Ausführung des Verfahrens umfasst.

[0080] Mobilität ist ein offensichtlicher und signifikanter Vorteil der Verwendung eines mobilen Geräts. Mit der Fähigkeit, das Verfahren auf einem mobilen Gerät auszuführen, können Benutzer von überall und jederzeit auf ihre Dokumente zugreifen und sie verarbeiten. Dies eröffnet neue Möglichkeiten für die Arbeit unterwegs, zu Hause oder in entfernten Standorten und ermöglicht eine größere Flexibilität in der Arbeitsweise.

[0081] Die Bequemlichkeit der Verwendung eines mobilen Geräts ist ein weiterer wesentlicher Vorteil. Mobile Geräte sind in der Regel intuitiv zu bedienen und bieten eine benutzerfreundliche Schnittstelle. Ausserdem sind die meisten Menschen bereits mit der Nutzung mobiler Geräte im täglichen Leben vertraut, was die Lernkurve für die Nutzung des Verfahrens reduziert. Darüber hinaus tragen mobile Geräte aufgrund ihrer Grösse und Portabilität dazu bei, die Benutzererfahrung bequem und nahtlos zu gestalten.

[0082] Die erfindungsgemässe Lösung weist auch ein Computersystem auf, dass Mittel zur Ausführung des Verfahrens umfasst.

[0083] Ein solches Computersystem steigert die Effizienz, da ein solches System die Arbeitsprozesse optimiert und seine Ressourcen effizienter nutzen kann. Die Konzentration auf spezifische Aufgaben erlaubt es dem System, die Leistung zu maximieren, was schnellere Bearbeitungszeiten, weniger Fehler und eine gesteigerte Produktivität zur Folge hat.

[0084] Darüber hinaus erhöht die Verwendung eines spezialisierten Computersystems die Anpassungsfähigkeit des Verfahrens. Es ermöglicht die Anpassung des Systems an spezifische Anforderungen und Arbeitsabläufe und bietet somit eine grössere Flexibilität und massgeschneiderte Lösungen, die auf die individuellen Bedürfnisse der Benutzer zugeschnitten sind. Das System kann entsprechend konfiguriert werden, je nachdem, ob es beispielsweise um die Anpassung der Benutzeroberfläche, spezielle Berichtsfunktionen oder bestimmte Verarbeitungsprozesse geht.

[0085] Für den Fachmann ist es selbstverständlich, dass alle beschriebenen Ausführungsformen in einer erfindungsgemässen Ausgestaltung der vorliegenden Erfindung verwirklicht sein können, sofern sie sich nicht explizit gegenseitig ausschliessen.

[0086] Im Folgenden wird die vorliegende Erfindung nun anhand konkreter Ausführungsbeispiele und Figuren näher erläutert, ohne jedoch auf diese beschränkt zu sein.

[0087] Durch das Studium dieser besonderen Ausführungsformen und Figuren können sich für einen Fachmann weitere vorteilhafte Ausführungen der vorliegenden Erfindung ergeben.

Figurenbeschrieb

[0088] Anhand der nachfolgenden Figuren werden Ausführungsbeispiele der Erfindung beschrieben. Es zeigen

Fig. 1: ein Diagramm des Anmeldens eines Benutzers;

Fig. 2: ein Diagramm der Dokumentenerfassung;

Fig. 3: ein Diagramm der Auflageneinforderung;

Fig. 4: ein Flussdiagramm des Erfassungsprozesses.

Ausführung der Erfindung

[0089] Figur 1 zeigt ein Diagramm des Anmeldens eines Benutzers. Dies stellt den ersten Schritt des Verfahrens zum Erfassen, Hochladen und Verarbeiten von Dokumenten 5 dar. Vorab sollte der Benutzer im Besitz eines Endbenutzergeräts 1 sein, welches in diesem Fall ein mobiles Gerät oder kurz Mobilgerät ist. Der Benutzer meldet sich in einer Applikation auf einem Server 3 an. Danach werden dem Benutzer Auswahllisten bereitgestellt, die es ihm ermöglichen, sein bevorzugtes Steuerjahr, eine Liste von Mandaten und den gewünschten Kanton festzulegen. In diesem konkreten Beispiel hat der Benutzer die Auswahl aus mehreren Kantonen und wählt dabei zum Beispiel den Kanton Obwalden aus. Aufgrund des ausgewählten Kantons wird ein Identitätsanbieter 4 aufgerufen, um den Benutzer zu authentifizieren. Anschliessend werden dem Benutzer die für ihn autorisierten Mandanten aufgelistet. Nachdem er einen ausgewählt hat, kann er weitere Funktionen nutzen. Das gesamte Verfahren wird an diese spezifischen Angaben angepasst.

[0090] Die Identifizierungsverfahren können variieren und sind von den Betreibern der Applikation festgelegt. In diesem Beispiel ist es eine Zwei-Faktor-Authentifizierung mit einer freiwilligen biometrischen Authentifizierung. Schliesslich wird nach erfolgreicher Identifizierung ein gültiges Zertifikat 2 an ein Mobilgerät 1 des Benutzers zurückgesendet.

[0091] Figur 2 präsentiert ein Diagramm der Dokumentenerfassung. In diesem Prozess greift der authentifizierte Benutzer mit seinem Endbenutzer- oder Mobilgerät 1 auf einen kantonalen Server 3 zu, um eine Liste von Mandanten zu erhalten. Im Anschluss daran kann der Benutzer die zugehörigen Dossiers für jeden einzelnen Mandanten anfragen und erhalten. Als nächstes beginnt der Prozess des Einscannens eines bestimmten Dokuments 5, in diesem Beispiel handelt es sich um einen Lohnausweis. Mit Hilfe, der auf dem Mobilgerät 1 installierten Applikation wird der Lohnausweis gescannt und anschliessend zur Signierung an eine signierende Stelle 6 gesendet. Schliesslich wird das signierte Dokument 5, also der Lohnausweis, zusammen mit einer Dokumentattributisierung 13, welche die Dokumentkategorie „Lohnausweis“ enthält, an den kantonalen Server zurückgesendet. Die Dokumentattributisierung repräsentiert in diesem Kontext die vom Benutzer ausgewählte Dokumentkategorie.

[0092] Figur 3 veranschaulicht ein Diagramm der Auflageneinforderung. Die Funktion der Auflageeinforderung besteht darin, den Benutzer darauf hinzuweisen, dass für die Fortführung bestimmter Prozesse, etwa der Veranlagung einer Steuer, noch nicht alle erforderlichen Unterlagen vorhanden sind. Beispielsweise überprüft die Kantonale Steuerverwaltung (KSTV) die von Benutzer eingereichte Steuererklärung und stellt fest, dass bestimmte Dokumente 5, wie ein Lohnausweis oder Säule 3a Nachweisdokumente, fehlen. Daraufhin erstellt die KSTV eine sogenannte Auflage und fordert die fehlenden Dokumente ein. Im Bestreben, den Prozess so papierlos wie möglich zu gestalten, soll die gesamte Kommunikation elektronisch ablaufen. Dazu informiert die KSTV den Benutzer über die Erstellung der Auflage, beispielsweise per E-Mail oder mittels einer Push-Benachrichtigung direkt auf das Mobiltelefon des Benutzers.

[0093] Daraufhin scannt oder fotografiert der Benutzer das geforderte Dokument 5 und lässt es an einer Signierende Stelle 6 signieren. Schliesslich wird das Dokument 5 an den kantonalen Server 3 übermittelt und die KSTV wird über dessen Einreichung informiert.

[0094] Figur 4 stellt ein Flussdiagramm des Erfassungsprozesses dar, in dem mehrere Schritte durchgeführt werden. Zunächst wird ein Dokument 5, beispielsweise ein papierbasierter Lohnausweis, als digitales Bild erfasst, was als Dokumentaufnahme 7 zu bezeichnen ist, und vorübergehend gespeichert. Dies kann die Erfassung einer oder mehrerer Seiten beinhalten, gefolgt von einer Perspektivenkorrektur und einer Bildoptimierung hinsichtlich Kontrasts, Schärfe und dergleichen. Darüber hinaus erfolgt die Datenextraktion und eventuell eine Dokumentaufnahmeüberprüfung 8 der Bildqualität durch den Benutzer. Sobald alle Seiten erfasst sind, erfolgt eine Dokumentaufnahmebestätigung 9 vom Benutzer. Die folgenden Schritte laufen dann automatisch ab. Aus dem erfassten Bild wird ein PDF-Dokument durch PDF-Datei-Generierung 10 erstellt, welches anschliessend mit dem Schritt des digitalen Signierens 11 signiert wird, um ein signiertes Dokument zu erzeugen. Diese Signatur kann innerhalb der einer signierenden Stelle 6 durchgeführt werden. Das signierte Dokument 5 wird dann an den Server 3 mit einer Serverübermittlung 12 übermittelt. Nach erfolgreicher Übermittlung an den Server 3 werden alle Daten aus dem Erfassungsprozess (Bild, PDF, signiertes PDF) vom Endbenutzergerät 1, beispielsweise von einem Tablet, gelöscht. Aus Nachvollziehbarkeitsgründen kann der Hash der Signatur auf dem Endbenutzergerät 1 gespeichert bleiben. Optional kann das Dokument 5 anschliessend mit fachlichen Angaben versehen werden, und zwar mittels einer Dokumentattributisierung 13. In diesem Fall wählt der Benutzer die Dokumentkategorie „Lohnausweis“. Die Dokumentattributisierung kann auch ausserhalb der Scan-Anwendung erfolgen, beispielsweise in der zugehörigen Webanwendung im Browser eines anderen Endbenutzergeräts 1.

[0095] In einer weiteren Ausführungsform umfasst das Verfahren die folgenden Schritte: Anmelden des Benutzers, Bereitstellen von Auswahllisten, Erfassen eines Dokuments, Signieren eines Dokuments, Übertragung des Dokuments an einen Server, Überprüfen des Dokuments durch den Server, und Freigabe zur Weiterverarbeitung.

[0096] Das Anmelden des Benutzers erfolgt gegenüber einer serverseitigen Applikation. Die Authentifizierung kann über verschiedene Wege erfolgen und wird meist durch den Betreiber der Applikation festgelegt. Die Identifikation des Benutzers ist relevant für die folgenden Schritte.

[0097] Angemeldeten Benutzern können Auswahllisten zur Verfügung gestellt werden. Beispiele für Auswahllisten sind Mandanten oder Steuerperioden. Diese sind beispielsweise relevant, damit ein Benutzer wählen kann, für welchen Mandanten und in welchem Steuerjahr dieser interagieren möchte. Die oben genannte Auflistung von Auswahllisten ist nicht abschliessend, grossmehrheitlich betreffen diese fachliche Aspekte.

[0098] Das Erfassen eines Dokuments umfasst, aus einem Bild ein signiertes PDF-Dokument zu generieren. Die Erfassung des Bildes kann mit Hilfe einer Mobilkamera direkt aus der Applikation oder Anwendung erfolgen oder es kann eine zuvor aufgenommene Bilddatei ausgewählt werden. Um den Zugriff auf allfällig sensitive Daten auf dem Endbenutzergerät zu minimieren werden jegliche Daten in einer Scan-Applikation in einer Sandbox gespeichert. Alle Bild-Daten werden im Rahmen des Erfassungsprozesses nur flüchtig gespeichert und nach dem Abschluss der Erfassung gelöscht. Ein Benutzer kann eine oder mehrere Bilder (häufig repräsentiert durch einzelne Seiten eines papiernen Dokuments) erfassen.

[0099] Nach der Auswahl oder der Aufnahme eines Bildes optimiert die Applikation das Bild, um die Lesbarkeit des Inhalts zu optimieren. Dies kann Perspektivenkorrekturen, Drehen und Schneiden des Bildinhalts, Änderungen des Kontrastwerts, Schärfen des Bildinhalts und weitere Optimierungen umfassen. Nachdem der Bildinhalt optimiert ist, wird dieser dem Benutzer zur Prüfung visualisiert und muss möglicherweise bestätigt werden. Nach erfolgreicher Quittierung wird aus dem Bild eine PDF-Datei generiert, welche anschliessend signiert wird.

[0100] Das Signieren eines Dokuments beinhaltet die Signatur des PDFs, welches im vorherigen Schritt generiert wurde. Die Signierung kann innerhalb der Applikation oder durch eine externe Signierungsstelle erfolgen. Das Resultat der Signierung ist eine signierte Datei, beispielsweise ein PDF-A Dokument. Dank der Signierung können allfällige Mutation am Inhalt erkannt werden. Im Verfahren ist dies relevant, um allfällige Mutationen durch einen „man in the middle“ auf Serverseite zu erkennen.

[0101] Als nächster Schritt erfolgt die Übertragung des Dokuments an den Server. Die initiale Anmeldung des Benutzers in der Applikation erlaubt der Scan-Applikation mit dem Server-Backend zu kommunizieren. Die signierte Datei wird in einem verschlüsselten Kanal, sicher an das Server-Backend übermittelt.

[0102] Schliesslich erfolgt das Überprüfen des Dokuments und Freigabe zur Weiterverarbeitung. Das Server-Backend prüft den empfangenen Inhalt und gibt der Scan-Applikation eine resultatbasierte Rückmeldung zurück.

OK (in Ordnung): Sofern der empfangene Inhalt in Ordnung ist, wird das Dokument zur weiteren Verarbeitung freigegeben. Der Scan-Applikation wird der erfolgreiche Empfang mitgeteilt, woraufhin diese die flüchtig gespeicherten Daten löscht. Möglicherweise wird für die Nachvollziehbarkeit ein Hash der signierten Datei auf dem Endbenutzergerät gespeichert (Sandbox).

NOK (nicht in Ordnung): Ist der Inhalt nicht in Ordnung, bspw. ungültige Signatur, wird der Inhalt serverseitig verworfen. Die Scan-Applikation erhält eine entsprechende Rückmeldung, agiert je nach Fehler unterschiedlich und informiert den Benutzer.

[0103] Ein weiteres Ausführungsbeispiel hierzu ist, beim Ausfüllen der Steuererklärung ein papierenes Dokument als elektronische Beilage für eine Steuererklärung zu erfassen. Das Folgende erläutert eine Ausprägung dieses beispielhaften Anwendungsfalles. Benutzer X ist eine natürliche Person und füllt seine Steuererklärung (NP) aus. Beim Erfassen des Einkommens wird der Lohnausweis als Pflichtbeilage angegeben. Dem Benutzer X liegt der Lohnausweis aber nur in papierener Form vor. Der Benutzer wird darauf aufmerksam gemacht, dass Beilagen auch mit dem Mobiltelefon erfasst werden können, und startet eine Scan-Applikation.

- I. Benutzer X startet die Scan-Applikation.
- II. Nach dem Einloggen werden jene Mandanten dargestellt, für die der Benutzer X berechtigt ist.
- III. Mit der Wahl des Mandanten werden die zugehörigen Steuerelemente beim Server abgefragt und in der Scan-Applikation dargestellt.
- IV. Nach der Wahl des gewünschten Dokuments kann der Benutzer Beilagen erfassen.
- V. Der Benutzer startet den Erfassungsprozess, wobei die folgenden Aktionen erfolgen können.
 - a. Aufnahme des papiernen Lohnausweises als digitales Bild (flüchtige Speicherung)
 - i. Erfassung von einer oder mehreren Seiten

- ii. Perspektivenkorrektur Bildoptimierung (Kontrast, Schärfe, etc.)
- iii. Datenextraktion
- b. Allfällige Überprüfung der Bildqualität durch Benutzer
- c. Sobald alle Seiten aufgenommen sind, wird dies durch den Benutzer bestätigt. Die nachfolgenden Schritte laufen weitgehend automatisiert ab.
- d. Anschliessend wird aus dem Bild ein PDF-Dokument generiert.
- e. Das generierte PDF wird digital signiert, woraus ein „Signiertes Dokument“ entsteht.
 - i. Die Signatur kann innerhalb der Applikation oder durch eine Signierungsstelle erfolgen.
- f. Das signierte Dokument wird an den Server übermittelt.
 - i. Bei erfolgreicher Übermittlung an den Server werden alle Daten aus dem Erfassungsprozess (Bild, PDF, signiertes PDF) vom mobilen Endgerät gelöscht. Aus Nachvollziehbarkeitsgründen könnte der Hash der Signatur noch auf dem Endgerät gespeichert werden.
- g. (optional) Danach kann das Dokument mit fachlichen Angaben dokumentattributiert werden. In diesem Falle wählt der Benutzer die Dokumentkategorie „Lohnausweis“. Die Dokumentattributierung kann auch ausserhalb der Scan-Applikation, beispielsweise in der zugehörigen Webapplikation im Browser eines anderen Geräts, erfolgen.

[0104] Mit den offenbarten Verfahren kann eine sichere und manipulationsfreie Übertragung von Dokumenten sichergestellt werden.

[0105] Die vorliegende Offenbarung bezieht sich auf ein Verfahren zum Erfassen, Hochladen und Verarbeiten von Dokumenten. Es versteht sich von selbst, dass für einen Fachmann zahlreiche weitere Ausführungsformen anhand der exemplarisch beschriebenen Ausführungsbeispiele denkbar sind.

Bezugszeichenliste

[0106]

- 1 Endbenutzergerät
- 2 Zertifikat
- 3 Server
- 4 Identitätsanbieter
- 5 Dokument
- 6 Signierende Stelle
- 7 Dokumentaufnahme
- 8 Dokumentaufnahmeüberprüfung
- 9 Dokumentaufnahmebestätigung
- 10 PDF-Datei-Generierung
- 11 Digitales Signieren
- 12 Serverübermittlung
- 13 Dokumentattributisierung

Patentansprüche

1. Verfahren zum Erfassen, Hochladen und Verarbeiten von Dokumenten (5), wobei das Verfahren die folgenden Schritte umfasst:
 - Anmelden eines Benutzers auf einem Endbenutzergerät (1), das mit einem Server (3) datentechnisch verbunden ist;
 - Vornahme einer Dokumentattributisierung (13);
 - Erfassen eines Dokuments (5);
 - Signieren des erfassten Dokuments (5);
 - Senden des erfassten signierten Dokuments (5) an den Server (3); und
 - Überprüfen des erfassten signierten Dokuments (5), wobei bei positiver Prüfung das Dokument (5) zur Verarbeitung freigegeben wird.
2. Verfahren gemäss Anspruch 1, ferner umfassend: basierend auf der Dokumentattributisierung eine Kategorisierung des Dokuments (5), und/oder erfassten Dokuments (5), und/oder erfassten signierten Dokuments (5).
3. Verfahren gemäss Anspruch 1 oder 2, wobei das Erfassen des Dokuments (5) eine Bildbearbeitung, insbesondere eine Perspektivenkorrektur und/oder eine Kontrastoptimierung und/oder eine Datenextraktion umfasst.

4. Verfahren gemäss einem der Ansprüche 1 bis 3, wobei die Vornahme der Dokumentattributisierung (13) in Erwiderung auf das Anmelden erfolgt.
5. Verfahren gemäss einem der Ansprüche 1 bis 4, ferner umfassend: Abfragen von auf dem Server (3) gespeicherten Dokumenten (5).
6. Verfahren gemäss einem der Ansprüche 1 bis 5, wobei das Dokument (5) und/oder erfasste Dokument (5), und/oder erfasste signierte Dokument (5) auf dem Endbenutzergerät (1) flüchtig gespeichert werden/wird.
7. Verfahren gemäss einem der Ansprüche 1 bis 6, wobei nach dem Senden des erfassten signierten Dokuments (5) an den Server (3) das Dokument (5) und/oder erfasste Dokument (5), und/oder erfasste signierte Dokument (5) auf dem Endbenutzergerät (1) nach positiver Prüfung ganz oder teilweise gelöscht werden/wird.
8. Verfahren gemäss einem der Ansprüche 1 bis 7, ferner umfassend: Aktualisieren einer Liste der an den Server (3) gesendeten Dokumenten (5) auf dem Endbenutzergerät (1).
9. Verfahren gemäss einem der Ansprüche 1 bis 8, wobei das Signieren des erfassten Dokuments (5) Metadaten umfasst.
10. Verfahren gemäss einem der Ansprüche 1 bis 9, wobei das Signieren des erfassten Dokuments (5) durch eine separate Komponente oder eine externe Komponente erfolgt.
11. Verfahren gemäss einem der Ansprüche 1 bis 10, wobei nach positiver Prüfung des erfassten signierten Dokuments (5), das erfasste signierte Dokument (5), und/oder die Kategorisierung, und/oder die zugehörigen Metadaten auf dem Server (3) gespeichert werden/wird.
12. Verfahren gemäss einem der Ansprüche 1 bis 11, ferner umfassend: Signaturspeicherung des erfassten signierten Dokuments (5) auf dem Endbenutzergerät (1) und/oder Server (3).
13. Verfahren gemäss einem der Ansprüche 1 bis 12, wobei die Prüfung des erfassten signierten Dokuments (5) eine Konsistenz- und/oder Integritätsprüfung umfasst.
14. Verfahren gemäss einem der Ansprüche 1 bis 13, wobei die Prüfung des erfassten signierten Dokuments (5) auf dem Server erfolgt.
15. Mobiles Gerät, umfassend Mittel zur Ausführung des Verfahrens nach einem der Ansprüche 1 bis 14.
16. Computersystem, umfassend Mittel zur Ausführung des Verfahrens nach einem der Ansprüche 1 bis 14.

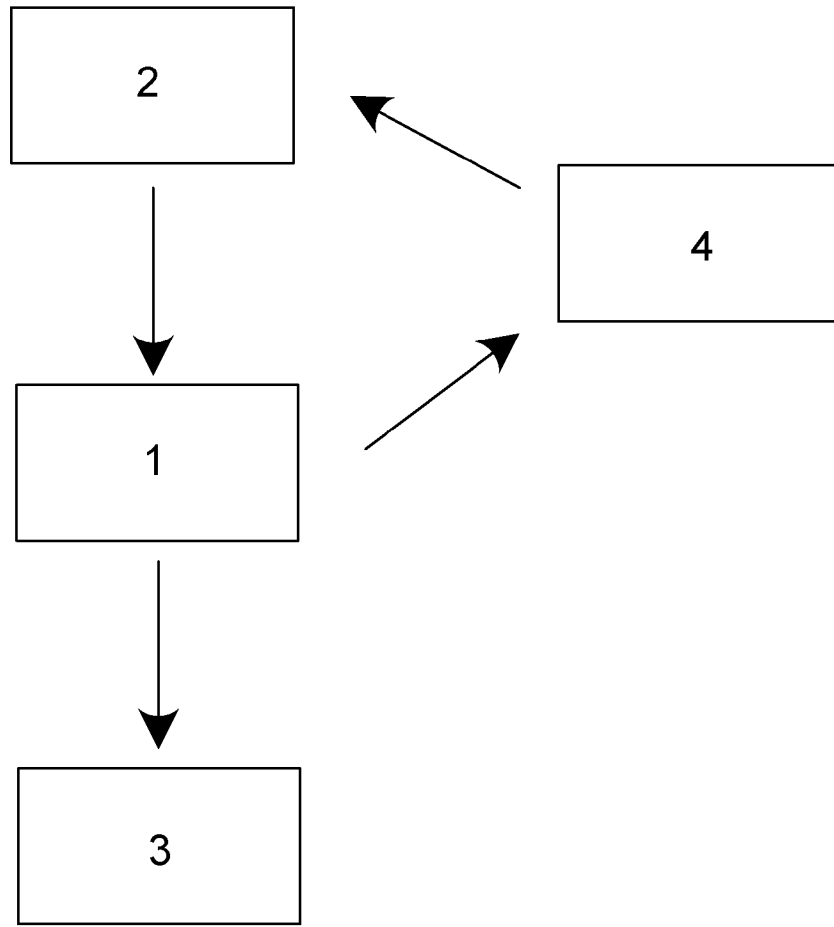


Fig. 1

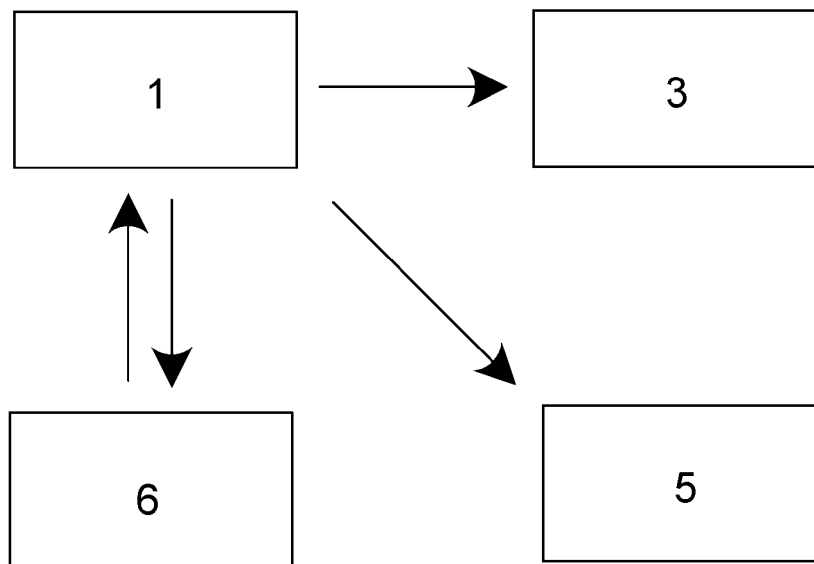


Fig. 2

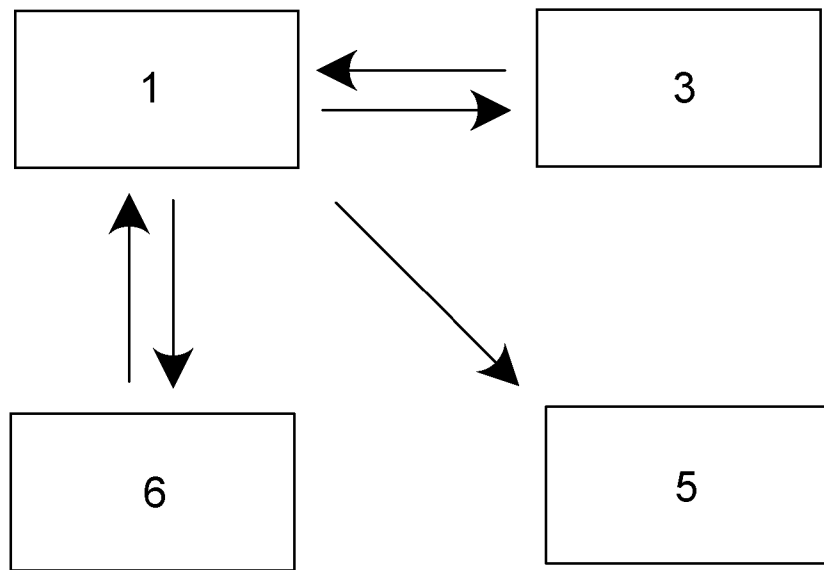


Fig. 3

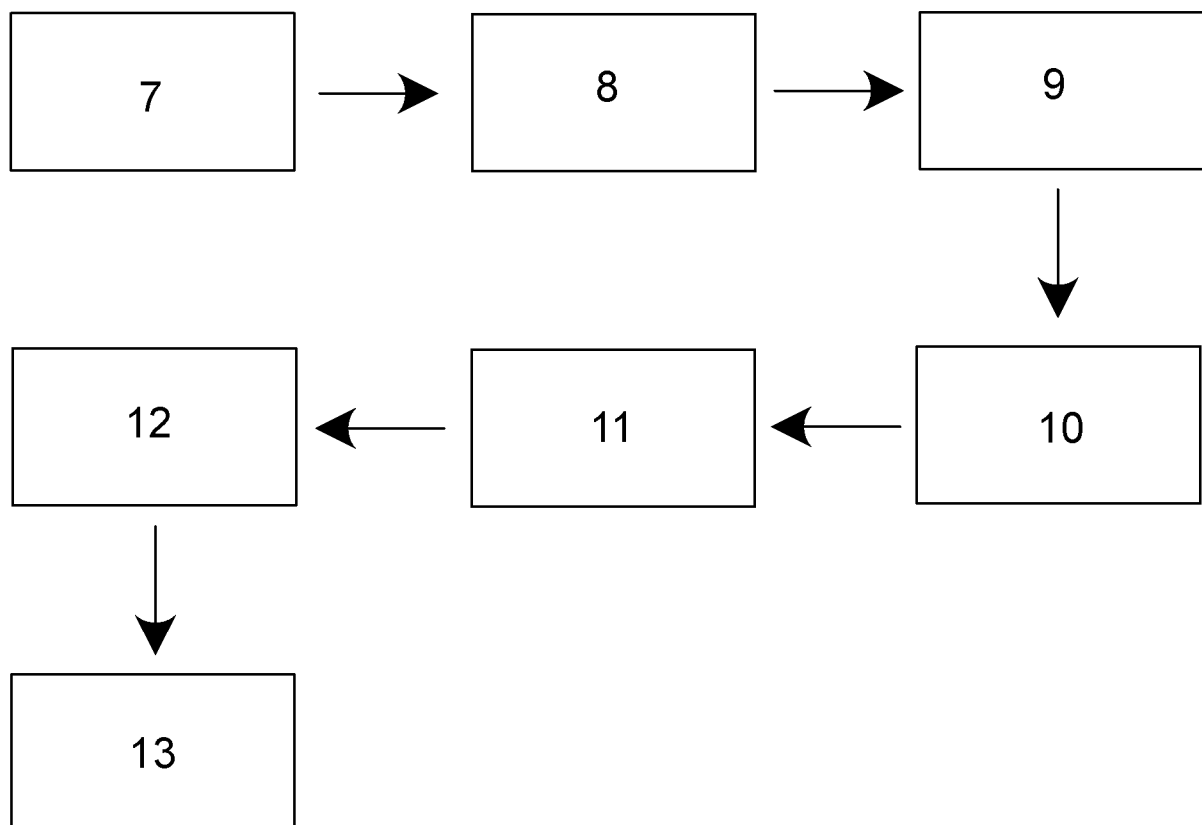


Fig. 4

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

KENNZEICHNUNG DER NATIONALEN ANMELDUNG	AKTENZEICHEN DES ANMELDERS ODER ANWALTS
	P101345CH
Nationales Aktenzeichen	Anmeldedatum
7252023	07-07-2023
Anmeldeland	Beanspruchtes Prioritätsdatum
CH	
Anmelder (Name)	
KMS AG	
Datum des Antrags auf eine Recherche Internationaler Art	Nummer, die die internationale Recherchenbehörde dem Antrag auf eine Recherche internationaler Art zugeteilt hat
05-09-2023	SN84635
I. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDS (treffen mehrere Klassifikationssymbole zu, so sind alle anzugeben)	
Nach der internationalen Patentklassifikation (IPC) oder sowohl nach der nationalen Klassifikation als auch nach der IPC	
Siehe Recherchenbericht	
II. RECHERCHIERTE SACHGEBIETE	
Recherchierter Mindestprüfstoff	
Klassifikationssystem	Klassifikationssymbole
IPC	Siehe Recherchenbericht
Recherchierte, nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Sachgebiete fallen	
III. ☐ EINIGE ANSPRÜCHE HABEN SICH ALS NICHT RECHERCHIERBAR ERWIESEN (Bemerkungen auf Ergänzungsbogen)	
IV. ☐ MANGELNDE EINHEITLICHKEIT DER ERFINDUNG (Bemerkungen auf Ergänzungsbogen)	

Formblatt PCT/ISA 201 A (11/2000)

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Nr. des Antrags auf Recherche

CH 7252023

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES		
INV.	G06F21/62	G06F21/64
		G06Q50/18
		H04L9/40
ADD.	G06F21/16	
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK		
B. RECHERCHIERTE SACHGEBIETE		
Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)		
G06F G06Q H04L		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)		
EPO-Internal, WPI Data		
C. ALS WESENTLICH ANGESEHENE VERÖFFENTLICHUNGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2021/049288 A1 (LI ZHIGUO [CN]) 18. Februar 2021 (2021-02-18) * Absätze [0006] - [0010], [0046], [0060] - [0061], [0063], [0070], [0076], [0078] - [0079], [0083] * * Absätze [0106] - [0119], [0123], [0131], [0160] - [0162], [0184], [0188], [0196] * * Absätze [0204], [0222] *	1-16
X	US 2019/026709 A1 (BARON CHARLES [US]) 24. Januar 2019 (2019-01-24) * Absätze [0002] - [0003], [0012] - [0019], [0021] - [0022], [0024], [0027], [0030] - [0032], [0035], [0040], [0042], [0044] - [0047] * ----- -/-	1-16
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" älteres Dokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll, oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des tatsächlichen Abschlusses der Recherche internationaler Art		Absendedatum des Berichts über die Recherche internationaler Art
5. Dezember 2023		
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Betz, Sebastian

Formblatt PCT/ISA/201 (Blatt 2) (Januar 2004)

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Nr. des Antrags auf Recherche

CH 7252023

C.(Fortsetzung). ALS WESENTLICH ANGESEHENE VERÖFFENTLICHUNGEN		
Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Bez. Anspruch Nr.
X	US 2022/405409 A1 (CHENG-SHORLAND CHAO [US] ET AL) 22. Dezember 2022 (2022-12-22) * Absätze [0004] - [0007], [0010] - [0011], [0040], [0044] - [0046], [0048] - [0050], [0058] - [0059], [0098] - [0103], [0156] - [0158] * -----	1-16

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Nr. des Antrags auf Recherche

CH 7252023

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2021049288 A1	18-02-2021	CN 111108522 A	05-05-2020
		SG 11202002395U A	29-04-2020
		US 2021049288 A1	18-02-2021
		US 2021342464 A1	04-11-2021
		WO 2019228549 A2	05-12-2019
US 2019026709 A1	24-01-2019	CN 104040543 A	10-09-2014
		EP 2803010 A1	19-11-2014
		US 2013269006 A1	10-10-2013
		US 2017024711 A1	26-01-2017
		US 2018232711 A1	16-08-2018
		US 2019026709 A1	24-01-2019
		US 2022156706 A1	19-05-2022
		WO 2013105941 A1	18-07-2013
US 2022405409 A1	22-12-2022	JP 2023001908 A	06-01-2023
		US 2022405409 A1	22-12-2022