(19) Deutsches Patent- und Markenamt

(10) **DE 10 2019 101 195 A1** 2020.07.23

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2019 101 195.7**
(22) Anmeldetag: **17.01.2019**
(43) Offenlegungstag: **23.07.2020**

(51) Int Cl.: ***H04L 9/00*** (2006.01)
H04L 9/14 (2006.01)
G06F 21/62 (2013.01)

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(74) Vertreter:
GLAWE DELFS MOLL Partnerschaft mbB von Patent- und Rechtsanwälten, 20148 Hamburg, DE

(72) Erfinder:
Schnjakin, Maxim, Dr., 10245 Berlin, DE;
Graupner, Hendrik, 14050 Berlin, DE

(56) Ermittelter Stand der Technik:

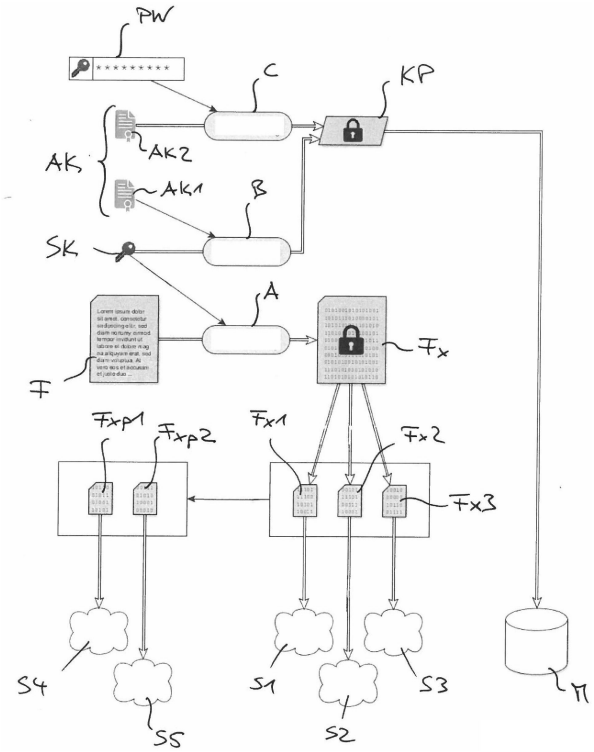
DE	**10 2014 113 430**	**A1**
US	**8 127 149**	**B1**
US	**8 762 712**	**B1**
US	**2014 / 0 068 262**	**A1**
US	**2014 / 0 215 210**	**A1**
US	**2015 / 0 113 279**	**A1**
US	**2016 / 0 142 382**	**A1**
US	**2018 / 0 034 630**	**A1**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zum sicheren Übermitteln einer Datei**

(57) Zusammenfassung: Verfahren zum sicheren Übermitteln einer Datei (F) zwischen einer ersten Rechnereinrichtung (100), die zu einer sicheren Übertragung von Dateien eingerichtet ist, und einer zweiten Rechnereinrichtung (200), die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform (P), mit
einer symmetrischen Verschlüsselung (A) einer zu übermittelnden Datei (F) mit einem symmetrischen Dateischlüssel (SK), und
einer asymmetrischen Verschlüsselung (B) des zufällig generierten Dateischlüssels (SK) mit dem öffentlichen Schlüssel (AK1) eines asymmetrischen Schlüsselpaares (AK) aus öffentlichem Schlüssel (AK1) und privatem Schlüssel (AK2).



Beschreibung

Technisches Gebiet

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum sicheren Übermitteln einer Datei zwischen einer ersten Rechnereinrichtung und einer zweiten Rechnereinrichtung über eine cloudbasierte Plattform.

Beschreibung des Standes der Technik

[0002] Datenaustausch findet im Unternehmensumfeld in der Regel per E-Mail (unverschlüsselt) oder über unsichere sogenannte Cloud-Plattformen statt. Aus dem Stand der Technik sind verschiedene Verfahren zur Speicherung von Nutzerdaten mittels eines oder mehrerer externer Speicherdienste bekannt, wie z.B. „OneDrive“, „Dropbox“, „Google Drive“ und andere. Viele Cloud-Plattformen bieten die Möglichkeit, die Datei per Link in einer E-Mail zu versenden, falls der Empfänger kein Nutzer dieser Plattform ist. Allerdings sind die Inhalte dieser Links unverschlüsselt und jede andere Person, die Zugriff auf diesen Link bzw. diese E-Mail erlangt, kann ebenfalls den Inhalt herunterladen. Sichere Kanäle zum Empfangen von E-Mails sind noch seltener. In der Regel muss das Gegenüber aufgefordert werden, einen Kanal zum Versand einzurichten.

[0003] Bei einer Übermittlung verschlüsselter Dateien ist es notwendig, dass sämtliche am Dateienübermittlungsprozess beteiligten Nutzer über die notwendigen Programme zum Ver- und Entschlüsseln verfügen.

[0004] Die Anmelderin der vorliegenden Patentanmeldung bietet unter dem Namen „Bdrive“ eine hochsichere und hochverfügbare Cloud-Speicher-Lösung für Unternehmen an, die mit einem besonderen Sicherheitskonzept arbeitet, das auch in der der DE 10 2014 113 430 A1 beschrieben ist: Daten werden bereits auf den Geräten der Nutzer verschlüsselt und fragmentiert, bevor sie bei mehreren Storage-Providern gespeichert werden. Dieser Ansatz bietet einen sehr hohen Schutz vor Datenverlust und volle Datensouveränität für Unternehmen und Behörden verbunden mit einer äußerst einfachen Nutzung.

Zusammenfassung der Erfindung

[0005] Ausgehend hiervon werden erfindungsgemäß ein Verfahren mit den Merkmalen des Anspruchs 1, 7 bzw. 9 sowie ein Computerprogramm bzw. ein Computer zur Ausführung des Verfahrens mit den Merkmalen der Ansprüche 12 bzw. 13 vorgeschlagen.

[0006] Die Erkenntnis der Erfindung liegt darin begründet, einen sicheren Daten- bzw. Dateientausch zwischen einer ersten Rechnereinrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, und einer zweiten Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform mittels einer Verknüpfungsadresse (mithin eines Internet-Links) zu gewährleisten, indem eine mindestens zweistufige hybride Verschlüsselung basierend auf zufällig generierten Verschlüsselungselementen ggf. kombiniert mit einer kennwortbasierten symmetrischen Verschlüsselung angewendet wird. Die cloudbasierte Übermittlung kann in Verbindung mit einer Dateifragmentierung erfolgen.

[0007] Insbesondere kann es sich bei der Verschlüsselung der zu übermittelnden Datei um eine symmetrische Verschlüsselung anhand eines zufällig generierten symmetrischen Dateischlüssels handeln. Eine derartige Verschlüsselung ist dem Fachmann an sich bekannt, bspw. als sogenannte AES-Verschlüsselung (AES: Advanced Encryption Standard). Bei einem derartigen symmetrischen Verschlüsselungsverfahren ist der Schlüssel zum Ver- und Entschlüsseln identisch. Erfindungsgemäß wird der Schlüssel zufällig erzeugt.

[0008] Anschließend erfolgt eine Verschlüsselung des zu der ersten symmetrischen Verschlüsselung verwendeten, zufällig erzeugten symmetrischen Schlüssels, mittels einer asymmetrischen Verschlüsselung. Eine derartige asymmetrische Verschlüsselung ist dem Fachmann ebenfalls an sich bekannt, bspw. als sogenannte RSA-Verschlüsselung (RSA: Rivest, Shamir und Adleman), bei dem es sich um ein deterministisches asymmetrisches Kryptoverfahren handelt.

[0009] Unter einer Verknüpfungsadresse oder einem Internet-Link (kurz Link oder auch Hyperlink) ist typischerweise ein Querverweis (in einem Hypertext oder als URL) zu verstehen, der funktional einen Sprung zu einem Ziel wie bspw. einem anderen elektronischen Dokument, an eine andere Stelle innerhalb eines Dokuments oder einer Zieladresse im Internet ermöglicht. Wenn der Hyperlink ausgeführt wird, wird automatisch das darin angegebene Ziel aufgerufen. Im allgemeinen wird der Begriff auf das World Wide Web bezogen, in dem Hyperlinks einen Kernbestandteil darstellen. So können und werden Hyperlinks u.a. dazu genutzt, um Dateien auf einen Computer herunterzuladen.

[0010] Das erfindungsgemäße Vorgehen umfasst mindestens zwei Verschlüsselungsschritte: zunächst wird der Inhalt der zu übermittelnden Datei mittels eines symmetrischen Verfahrens mit einem zufällig generierten Dateischlüssel verschlüsselt. Dieser Dateischlüssel wird dann mittels eines asymmetrischen Verfahrens mit einem öffentlichen Schlüssel verschlüsselt.

[0011] Das erfindungsgemäße Vorgehen dient zur Übermittlung von Dateien zwischen einer ersten Rechnereinrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, und einer zweiten Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform. Dies kann zum einen den Fall umfassen, dass eine Datei von der zur sicheren Übertragung eingerichteten ersten Rechnereinrichtung an die nicht entsprechend eingerichtet zweite Rechnereinrichtung übermittelt wird, und zum anderen den umgekehrten Fall, wonach die Dateienübermittlung von der nicht zur sicheren Übertragung eingerichteten zweiten Rechnereinrichtung an die zum sicheren Empfang eingerichtete erste Rechnereinrichtung stattfindet. In beiden Konstellationen ermöglicht die Erfindung eine sichere Übermittlung, ohne dass entsprechende Einrichtungen auf der zweiten Rechnereinrichtung vorhanden sein müssten.

[0012] In beiden Fällen erfolgt die beschriebene zumindest zweistufige Hybridverschlüsselung und die Übermittlung der verschlüsselten Datei über eine cloudbasierte Plattform, wobei auch der zur Verschlüsselung der Datei verwendete und hernach asymmetrisch verschlüsselte symmetrische Schlüssel über die Plattform übermittelt wird.

[0013] Zudem kann in Weiterbildung der Erfindung eine kennwortbasierte Komponente hinzugefügt werden, die erfordert, dass sich die zweite Rechnereinrichtung beim Zugang zu der cloudbasierten Plattform (mithin bei der Ausführung der Verknüpfungsadresse) mittels eines von der ersten Rechnereinrichtung erhaltenen Kennworts legitimiert. In der erstgenannten Variante einer Übertragung einer zu übermittelnden Datei von der ersten Rechnereinrichtung an die zweite Rechnereinrichtung kann dies dadurch erreicht werden, dass der zugehörige private Schlüssel anhand eines kennwortbasierten symmetrischen Verfahrens verschlüsselt wird.

[0014] In beiden beschriebenen Varianten kann die übermittelnde Datei nach erfolgter Verschlüsselung fragmentiert und die so erhaltenen Fragmentdateien auf mehreren cloudbasierten Servern gespeichert werden.

[0015] Die vorliegende Beschreibung deckt auch ein Computerprogramm mit Programmcode ab, der dazu geeignet ist, ein erfindungsgemäßes Verfahren auszuführen, wenn das Computerprogramm auf einer geeigneten Rechnereinrichtung und/oder einem Zentralserver abläuft. Es werden sowohl das Computerprogramm selbst als auch abgespeichert auf einem computerlesbaren Medium (Computerprogrammprodukt) beansprucht.

[0016] Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen, der Beschreibung und den beiliegenden Zeichnungen.

[0017] Es versteht sich, dass die voranstehend genannten und die nachstehend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung, wie sie in den Ansprüchen definiert ist, zu verlassen.

[0018] Die Erfindung ist anhand von Ausführungsbeispielen in den Zeichnungen schematisch dargestellt und wird im folgenden unter Bezugnahme auf die Zeichnungen ausführlich beschrieben.

Figurenliste

Fig. 1 zeigt als schematisches Blockablaufdiagramm eine Ausführungsform des erfindungsgemäßen Verfahrens zum sicheren Übermitteln einer Datei von einer ersten Rechnereinrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine zweite Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform.

Fig. 2 zeigt eine weitere schematische Veranschaulichung des Verfahrens der **Fig. 1**.

Fig. 3 zeigt ein Sequenzdiagramm zur Erstellung eines Download-Links für das Verfahren der **Fig. 1** und **Fig. 2**.

Fig. 4 zeigt ein Sequenzdiagramm zum Ablauf des Verfahrens der **Fig. 1** und **Fig. 2**.

Fig. 5 zeigt als schematisches Blockablaufdiagramm eine weitere Ausführungsform des erfindungsgemäßen Verfahrens zum sicheren Übermitteln einer Datei von einer zweiten Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine erste Rechnereinrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform.

Fig. 6 zeigt eine weitere schematische Veranschaulichung des Verfahrens der **Fig. 5**.

Fig. 7 zeigt ein Sequenzdiagramm zur Erstellung eines Upload-Links für das Verfahren der **Fig. 5** und **Fig. 6**.

Fig. 8 zeigt ein Sequenzdiagramm zum Ablauf des Verfahrens der **Fig. 5** und **Fig. 6**.

Ausführliche Beschreibung

[0019] Anhand der **Fig. 1** bis **Fig. 4** wird im folgenden eine Variante der Erfindung beschrieben, bei der eine zu übermittelnde Datei von einer ersten Rechner-

einrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine zweite Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, übertragen wird. Anhand der **Fig. 5** bis **Fig. 6** wird ebenfalls im folgenden eine weitere Variante der Erfindung beschrieben, bei der eine zu übermittelnde Datei von einer zweiten Rechnereinrichtung, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine erste Rechnereinrichtung, die zu einer sicheren Übertragung von Dateien eingerichtet ist, übertragen wird. In beiden Fällen erfolgt die Übertragung über eine cloudbasierte Plattform. In beiden Fällen werden gleiche oder ähnliche Merkmale, Verfahrensschritte usw. mit gleichen Bezugszeichen bezeichnet.

[0020] **Fig. 1** zeigt eine zu übermittelnde Datei F, die von einer ersten Rechnereinrichtung **100**, die zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine zweite Rechnereinrichtung **200**, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, übertragen werden soll (vgl. auch **Fig. 2**).

[0021] Im dargestellten Beispiel will ein erster Nutzer **P1** mit dem Namen „Max Mustermann“ von seiner ersten Rechnereinrichtung **100** die Datei F an einen zweiten Nutzer **P2** mit dem Namen „Gerd Mueller“ senden. Der zweite Nutzer **P2** verfügt über die zweite Rechnereinrichtung **200**, die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist.

[0022] Auf der ersten Rechnereinrichtung **100** wird die zur Übermittlung ausgewählte Datei F anhand eines (zufällig erzeugten) symmetrischen Schlüssels **SK** verschlüsselt (vgl. Bezugszeichen **A**). Die so erzeugte verschlüsselte Datei Fx wird auf einem cloudbasierten Server abgespeichert. In dem dargestellten Ausführungsbeispiel wird die Datei zur Erhöhung der Sicherheit in an sich bekannter Art und Weise in Dateifragmente **Fx1**, **Fx2**, **Fx3** fragmentiert und die Fragmente **Fx1**, **Fx2**, **Fx3** werden auf jeweils einem cloudbasierten Server **S1**, **S2**, **S3** abgespeichert. Zudem können sogenannte Paritätsblöcke **Fxp1**, **Fxp2** der Fragmente erzeugt und auf weiteren (cloudbasierten) Servern **S4**, **S5** hinterlegt werden (dieses Vorgehen ist dem Fachmann als RAIC-Verfahren (redundante Anordnung unabhängiger Cloud-Speicher) bekannt und unter anderem in der DE 10 2014 113 430 A1 beschrieben). Aus Gründen der Übersichtlichkeit sind in der **Fig. 2** lediglich die Cloud-Speicher **S1**, **S2**, **S3** dargestellt.

[0023] Dann wird ein asymmetrisches Schlüsselpaar **AK** (zufällig) erzeugt, bestehend aus einem öffentlichen Schlüssel **AK1** und einem privaten Schlüssel **AK2**, und der symmetrische Schlüssel **SK** wird anhand des so erzeugten öffentlichen Schlüssels **AK1** verschlüsselt (vgl. Bezugszeichen **B**). Dieser verschlüsselte Schlüssel wird in einer zentralen Speichereinrichtung **M** (die ebenfalls der cloudbasierten Plattform **P** zugeordnet ist) abgespeichert.

[0024] Gemäß dem dargestellten Ausführungsbeispiel kann noch eine dritte Verschlüsselungsstufe vorgesehen sein, die darin besteht, den erzeugten privaten Schlüssel **AK2** mittels eines Kennwortes **PW** kennwortbasiert (symmetrisch) zu verschlüsseln (vgl. Bezugszeichen **C**). Die beiden bei **B** und **C** derart jeweils verschlüsselten Schlüssel **AK1**, **AK2** werden als sozusagen zweifach verschlüsseltes Schlüsselpaket **KP** dann auf der zentralen Speichereinrichtung **M** hinterlegt.

[0025] **Fig. 3** zeigt ein Sequenzdiagramm, das den Ablauf der Erfindung auf Seiten des ersten Nutzers, d.h. auf der ersten Rechnereinrichtung **100**, für eine Dateienübermittlung von der ersten Rechnereinrichtung **100** zu der zweiten Rechnereinrichtung **200** darstellt.

[0026] Auf der Rechnereinrichtung **100** laufen erfindungsgemäß die im folgenden beschriebenen Schritte ab. Bei **S10** wird durch den ersten Nutzer **P1** die zu übermittelnde Datei F ausgewählt und die für die Erstellung des Links (das heißt der Verknüpfungsadresse) **L** notwendigen Link-Daten werden erfasst. Bei den Link-Daten handelt es sich bspw. um eine Datei-Referenz, ggf. den kennwortverschlüsselten privaten Schlüssel **AK2** sowie ggf. ein Ablaufdatum für die Wirksamkeit des Links **L** (Verfallsdatum). Außerdem erfolgt bei **S10** die symmetrische Verschlüsselung **A** der Datei **F** durch einen zufällig generierten symmetrischen Schlüssel **SK**.

[0027] Soll die kennwortbasierte Verschlüsselung des privaten Schlüssels **AK2** vorgenommen werden, so wird bei **S11** das dafür notwendige optionale Kennwort **PW** eingegeben (die zwischen **S11** und **S10** eingezeichnete punktierte Verbindung deutet die manuelle Eingabe des Kennworts **PW** durch den Nutzer **P1** an).

[0028] Bei **S12** wird von der Rechnereinrichtung **100** ein zufälliges asymmetrisches Schlüsselpaar **AK** generiert. Liegt ein eingegebenes Kennwort **PW** vor, so wird bei S14 der private Schlüssel **AK2** des bei **S12** generierten asymmetrischen Schlüsselpaares **AK** mit dem eingegebenen Kennwort **PW** symmetrisch verschlüsselt.

[0029] Bei **S16** erfolgt die asymmetrische Verschlüsselung **B** des symmetrischen Schlüssels **SK** anhand des öffentlichen Schlüssels **AK1** des bei **S12** generierten asymmetrischen Schlüsselpaares **AK**.

[0030] Bei **S18** wird von der ersten Rechnereinrichtung **100** der Web-Link **L** angefordert. Hierzu sendet die Rechnereinrichtung **100** die bei **S10** erfassten Link-Daten an einen Service **150** der cloudbasier-

ten Plattform **P**, über die die Übermittlung der Datei **F** erfolgen soll. Unter dem Begriff „Service“ ist hierbei ein Computerprogramm bzw. eine Software zu verstehen, die auf einem hierzu eingerichteten Server der Plattform **P** implementiert ist. Der erste Nutzer **P1** kann zur Nutzung dieser Software, d.h. des Services **150**, über eine Internetanbindung auf den externen Server, bspw. mittels eines Webbrowsers, zugreifen.

[0031] Der Service **150** persistiert bzw. erzeugt bei **S20** den Link **L**, der bspw. folgende Form hat:

Link {

Datei-Referenz,

privater Schlüssel,

Ablaufdatum

}

[0032] Der so erzeugte Web-Link **L** wird von dem Service **150** bei **S21** an die Rechnereinrichtung **100** gesandt. Der erste Nutzer **P1** sendet den Link **L** bspw. und insb. per elektronischer Post / E-Mail **10** an die Rechnereinrichtung **200** des zweiten Nutzers **P2** (vgl. **Fig. 2**).

[0033] **Fig. 4** zeigt ein Sequenzdiagramm, das den Ablauf der Erfindung auf Seiten des zweiten Nutzers, d.h. auf der zweiten Rechnereinrichtung **200**, nach Erhalt des Links **L** darstellt.

[0034] Das Sequenzdiagramm der **Fig. 4** umfasst drei Ablaufspalten, ganz links ist der Ablauf auf der zweiten Rechnereinrichtung **200** gezeigt, in der Mitte der Ablauf auf dem Plattform-Service **150** und ganz rechts sind die cloudbasierten Server (oder Cloudserver) **S1**, **S2**, **S3** dargestellt.

[0035] Der zweite Nutzer **P2** gibt den erhaltenen Link **L** bei **S22** in seinen Webbrowser **30** ein (bspw. indem er auf den Link **L** klickt) und öffnet damit die damit verbundene Anwendung. Gegebenenfalls gibt der zweite Nutzer **P2** das notwendige Kennwort **PW** ein, mit dem der private asymmetrische Schlüssel **AK2** symmetrisch verschlüsselt wurde; das Kennwort **PW** wurde dem zweiten Nutzer **P2** von dem ersten Nutzer **P1** unabhängig von der Übersendung des Links **L** und vorzugsweise über einen andersartigen Kommunikationskanal ausgehändigt oder übermittelt, bspw. durch Überreichen einer Visitenkarte **20** oder einer anderen Notiz, auf der das Kennwort **PW** vermerkt ist.

[0036] Eine zu dem Link **L** gehörende Link-ID wird bei **S23** an den Service **150** übermittelt (die entsprechend im gegebenen Falle auch das Kennwort **PW** umfasst), und der Service **150** prüft die übermittelten Link-Daten bei **S24**. Wurde die Richtigkeit der Daten, insb. Kennwort **PW** und/oder Verfallsdatum, festgestellt, stellt der Service **150** bei **S26** den privaten Schlüssel **AK2** und sogenannte Cloud-Tokens zum Zugriff auf die Cloudserver **S1**, **S2**, **S3** zum Abrufen der zu übermittelnden Datei bereit, deren Übermittlung an die zweite Rechnereinrichtung **200** bei **S27** erfolgt.

[0037] Die übermittelten Cloud-Token werden von der zweiten Rechnereinrichtung **200** bei **S28** an die Cloudserver übermittelt, die bei **S29** die dort gespeicherten (verschlüsselten) Dateifragmente **Fx1**, **Fx2**, **Fx3** zur Verfügung stellen und bei **S30** an die zweite Rechnereinrichtung **200** übermitteln. Dort werden die (immer noch verschlüsselten) Dateifragmente bei **S32** zusammengesetzt und entschlüsselt (Entschlüsselung des übermittelten privaten Schlüssels **AK2** anhand des eingegebenen Kennworts **PW** und Anwenden des privaten Schlüssels **AK2**, um den mit dem öffentlichen Schlüssel **AK1** verschlüsselten symmetrischen Schlüssel **SK** zu entschlüsseln, um mit diesem wiederum die wieder zusammengesetzte verschlüsselte Datei Fx zu entschlüsseln.

[0038] Ist das Kennwort korrekt bzw. die Entschlüsselung erfolgreich, wird bei **S34** der lokale Download der entschlüsselten Datei **F** initiiert und die Rechnereinrichtung **200** (bzw. deren Nutzer **P2**) ist somit im Besitz der sicher übermittelten Datei **F**.

[0039] Das beschriebene dreistufige Verfahren bietet ein hohes Maß an Sicherheit, da es die jeweiligen Vorteile der drei einzelnen Verschlüsselungsverfahren kombiniert. Die symmetrische Verschlüsselung der zu übermittelnden Datei ist sehr performant und somit für große Datenmengen, wie sie bei zu übermittelnden Dateien (Präsentationen, Filme, Audiodateien, usw.) häufig auftreten, geeignet. Mit der asymmetrischen Verschlüsselung wird dem Gesamtprozess eine Asynchronität hinzugefügt, d.h. es können später Änderungen der Datei oder weitere Dateien hinzugefügt werden, ohne dass ein Klartextschlüssel oder -kennwort abgefragt werden muss. Da die asymmetrische Verschlüsselung „nur“ auf den symmetrischen Schlüssel angewendet wird, können keine Performanzprobleme auftreten. Der dritte (optionale) Aspekt der kennwortbasierten Verschlüsselung stellt eine Verschlüsselung mit einfach zu übertragendem Schlüssel (Aufschreiben, Diktieren am Telefon o.dgl.) dar.

[0040] **Fig. 7** zeigt ein Sequenzdiagramm, das den Ablauf der Erfindung auf Seiten des ersten Nutzers, d.h. auf der ersten Rechnereinrichtung **100**, für eine Dateienübermittlung von der zweiten Rechnereinrichtung **200** zu der ersten Rechnereinrichtung **100** darstellt. In dieser Variante wird dem Nutzer der zweiten Rechnereinrichtung **200** eine Möglichkeit zum sicheren Hochladen der Datei auf die Cloud-Plattform eingerichtet, um die zu übermittelnde Datei erfindungsgemäß sicher übertragen zu können.

[0041] Hierfür richtet der erste Nutzer **P1** von der ersten Rechnereinrichtung **100** aus einen Link zu einer Hochlademöglichkeit ein. Diese Hochlademöglichkeit soll der Einfachheit halber in der Folge kurz als „Droppad" bezeichnet werden. Bei **S40** erfasst der erste Nutzer **P1** die Daten für das Droppad; hierbei handelt es sich insb. um einen Namen und eine Beschreibung des Vorgangs sowie einen Pfad und einen öffentlichen Schlüssel **AK1**. Soll ein Kennwortschutz hinzugefügt werden, so gibt der erste Nutzer **P1** bei **S41** ein entsprechendes Kennwort **PW** ein. Bei **S40** wird dann ein Hashwert dieses Kennwortes berechnet und den Droppad-Daten hinzugefügt, die dann bei **S42** an den Plattform-Service **150** übermittelt.

[0042] Plattformseitig wird bei **S43** das Droppad erstellt/persistiert und ein Link **L** erzeugt, der bei **S44** an die erste Rechnereinrichtung **100** übermittelt wird. Der Droppad-Link kann bspw. folgende Form haben:

Droppad {

Name,

Beschreibung,

Pfad

(Kennworthash)

öffentl. Schlüssel,

Ablaufdatum

}

[0043] Wie in der zuvor beschriebenen ersten Variante sendet der erste Nutzer **P1** den Link **L** bspw. und insb. per elektronischer Post / E-Mail **10** an die Rechnereinrichtung **200** des zweiten Nutzers **P2** (vgl. **Fig. 6**).

[0044] **Fig. 8** zeigt ein Sequenzdiagramm, das den Ablauf der Erfindung auf Seiten des zweiten Nutzers, d.h. auf der zweiten Rechnereinrichtung **200**, nach Erhalt des Links **L** darstellt.

[0045] Ähnlich wie zuvor in der **Fig. 4** umfasst das Sequenzdiagramm der **Fig. 8** drei Ablaufspalten, ganz links ist der Ablauf auf der zweiten Rechnereinrichtung **200** gezeigt, in der Mitte der Ablauf auf dem Plattform-Service **150** und ganz rechts sind die cloudbasierten Server (oder Cloudserver) **S1**, **S2**, **S3** dargestellt.

[0046] Der zweite Nutzer **P2** gibt den erhaltenen Link **L** bei **S50** in seinen Webbrowser **30** ein (bspw. indem er auf den Link **L** klickt) und öffnet damit die damit verbundene Anwendung. Gegebenenfalls gibt der zweite Nutzer **P2** das notwendige Kennwort **PW** ein; das Kennwort **PW** wurde dem zweiten Nutzer **P2** von dem ersten Nutzer **P1** unabhängig bzw. separat von der Übersendung des Links **L** ausgehändigt oder übermittelt (vgl. oben).

[0047] Von dem ggf. eingegebenen Kennwort **PW** wird der Hashwert errechnet, und bei **S51** werden eine in dem Link **L** enthaltene Droppad-ID und der Kennworthashwert an den Service **150** übermittelt. Der Service **150** überprüft bei **S52** die Droppad-Daten und ggf. den Kennworthashwert (und/oder ggf. ein enthaltenes Verfallsdatum) und erzeugt - bei positivem Abgleich - bei **S54** sogenannte Autorisierungstoken, die bei **S55** an die zweite Rechnereinrichtung **200** übermittelt werden.

[0048] Dann wählt der zweite Nutzer **P2** bei **S56** eine zu übermittelnde Datei **F** aus, indem der sie in der auf einem Browser **30** seiner zweiten Rechnereinrichtung **200** ablaufenden Webanwendung öffnet oder sie per Drag-and-Drop hineinverschiebt/-kopiert. Dadurch wird eine (von den Autorisierungstoken autorisierte) Anfrage an den Service **150** gestartet (**S57**).

[0049] Auf die Anfrage stellt der Service **150** bei **S58** den öffentlichen Schlüssel **AK1** (von der ersten Rechnereinrichtung **100**, d.h. des ersten Nutzers **P1**) sowie einen oder mehrere sogenannte Cloud-Token zum Zugriff auf Cloudserver **S1**, **S2**, **S3** bereit. Bei **S59** werden die bereitgestellten Zertifikate an die zweite Rechnereinrichtung **200** übermittelt.

[0050] Bei **S60** erzeugt die Webanwendung auf der zweiten Rechnereinrichtung **200** einen zufälligen symmetrischen Schlüssel **SK** (alternativ kann der symmetrische Schlüssel bspw. von dem Service **150** erzeugt und übermittelt werden) und verschlüsselt mit dem symmetrischen Schlüssel **SK** die zu übermittelnde Datei **F** (vgl. auch Bezugszeichen **A** in **Fig. 5**). Die so erzeugte verschlüsselte Datei Fx kann dann wie dargestellt (**Fig. 5**) fragmentiert werden. Des weiteren wird der symmetrische Schlüssel **SK** asymmetrisch mit übermittelten öffentlichen Schlüssel **AK1** des ersten Nutzers **P1** verschlüsselt (vgl. wiederum auch **Fig. 5**, Bezugszeichen **B**). Der verschlüsselte Schlüssel **KP'** wird bei **S61** an den Service **150** übermittelt. Bei **S62** generiert der Service **150** entsprechende Metadaten (umfassend Namen, Schlüssel, u.a.m.), die zentral zum späteren Abgleich abgespeichert werden (bspw. Zentralspeicher **M**, vgl. **Fig. 5**).

[0051] Bei **S64** wiederum werden die Dateifragmente (oder nur die verschlüsselte Datei, falls keine Fragmentierung erfolgt) hochgeladen und bei **S65** zusammen mit den Cloud-Token an die Cloudserver **S1**, **S2**, **S3** übertragen, wo die Dateifragmente **Fx1**, **Fx2**, **Fx3** gespeichert werden (vgl. auch **Fig. 5** und **Fig. 6**). Wie in **Fig. 5** skizziert, kann selbstverständlich auch eine Paritätsblockbildung wie bereits im Zusammenhang mit der ersten Übertragungsvariante erfolgen.

[0052] Der erste Nutzer **P1** kann nach erfolgtem Hochladen der zu übermittelnden Datei anhand der Metadaten bzw. den Droppad-ID-Daten von dem Service **150** identifiziert und ggf. benachrichtigt werden, damit er unter dem ihm bekannten Pfad die zu übermittelnde Datei abruft und herunterlädt. Eine direkte Benachrichtigung des ersten Nutzers **P1** durch den zweiten Nutzer **P2** ist nicht notwendig.

[0053] Die Erfindung ermöglicht somit ein sicheres Versenden/Übermitteln von Daten bzw. Dateien, ohne dass für die beteiligten Nutzer ein erheblicher Mehraufwand entsteht. Erfindungsgemäß sind die Daten stark verschlüsselt, insbesondere bei der zusätzlichen beschriebenen Kennwortverschlüsselung, und können durch einfaches Mitlesen der elektronischen Post, mit der die Verknüpfungsadresse/der Link übermittelt wird, nicht eingesehen werden. Zudem kann auch ein „Einbruch“ beim Speicheranbieter nicht zur Offenlegung der in den abgespeicherten Dateien enthaltenen Daten führen, da sie dort nur verschlüsselt vorliegen und (bei Fragmentierung) bei einem Anbieter jeweils nur ein Bruchstück der Datei vorliegt. Der ganz besondere Vorteil der Erfindung liegt darin begründet, dass auch Personen an einem sicheren Datenaustausch teilnehmen können, die keine technischen Vorkehrungen zum sicheren Empfangen bzw. Versenden von Dateien getroffen haben.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102014113430 A1 [0004, 0022]

Patentansprüche

1. Verfahren zum sicheren Übermitteln einer Datei (F) zwischen einer ersten Rechnereinrichtung (100), die zu einer sicheren Übertragung von Dateien eingerichtet ist, und einer zweiten Rechnereinrichtung (200), die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform (P), mit
einer symmetrischen Verschlüsselung (A) einer zu übermittelnden Datei (F) mit einem symmetrischen Dateischlüssel (SK), und
einer asymmetrischen Verschlüsselung (B) des zufällig generierten Dateischlüssels (SK) mit dem öffentlichen Schlüssel (AK1) eines asymmetrischen Schlüsselpaares (AK) aus öffentlichem Schlüssel (AK1) und privatem Schlüssel (AK2).

2. Verfahren nach Anspruch 1, bei dem die zu übermittelnde Datei (F) nach erfolgter Verschlüsselung auf einem cloudbasierten Server gespeichert wird oder bei dem die zu übermittelnde Datei (F) nach erfolgter Verschlüsselung fragmentiert wird und die so erhaltenen Fragmentdateien (Fx1, Fx2, Fx3) auf mehreren cloudbasierten Servern (S1, S2, S3) gespeichert werden.

3. Verfahren nach Anspruch 1 oder 2, bei dem der zweiten Rechnereinrichtung (200) von der ersten Rechnereinrichtung (100) eine Verknüpfungsadresse (L) zum Hochladen oder Herunterladen einer zu übermittelnden Datei (F) durch die zweite Rechnereinrichtung (200) übermittelt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem das asymmetrische Schlüsselpaar (AK) auf der ersten Rechnereinrichtung (100) erzeugt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, des weiteren mit einer kennwortbasierten symmetrischen Verschlüsselung (C) des privaten Schlüssels (AK2) des zufällig generierten Schlüsselpaares (AK).

6. Verfahren nach Anspruch 5, bei dem die Verknüpfungsadresse (L) durch Eingabe des Kennwortes (PW) der kennwortbasierten Verschlüsselung (C) geöffnet und ausgeführt werden kann.

7. Verfahren zum sicheren Übermitteln einer Datei (F) von einer ersten Rechnereinrichtung (100), die zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine zweite Rechnereinrichtung (200), die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform (P), mit den folgenden Schritten auf der ersten Rechnereinrichtung (100):
- Bereitstellen einer zu übermittelnden Datei (F),
- Generieren eines symmetrischen Dateischlüssels (SK),
- symmetrisches Verschlüsseln (A) der zu übermittelnden Datei (F) mit dem symmetrischen Dateischlüssel (SK),
- Generieren eines asymmetrischen Schlüsselpaares (AK) aus öffentlichem Schlüssel (AK1) und privatem Schlüssel (AK2),
- asymmetrisches Verschlüsseln (B) des symmetrischen Dateischlüssels (SK) mit dem öffentlichen Schlüssel (AK1),
- Abspeichern der symmetrisch verschlüsselten Datei (Fx) auf mindestens einem der cloudbasierten Plattform (P) zugeordneten Speicher (S1, S2, S3),
- Übermitteln des asymmetrisch verschlüsselten symmetrischen Dateischlüssels (SK) an eine der cloudbasierten Plattform (P) zugeordnete Speichereinrichtung (M).

8. Verfahren nach Anspruch 7, mit den weiteren Schritten:
- Erzeugen eines Kennwortes (PW),
- symmetrisches Verschlüsseln (C) des privaten Schlüssels (AK2) mit dem Kennwort (PW) und dadurch Erzeugen eines zweifach verschlüsselten Schlüsselpakets (KP),
- Übermitteln des Schlüsselpakets (KP) an die der cloudbasierten Plattform (P) zugeordnete Speichereinrichtung (M) .

9. Verfahren zum sicheren Übermitteln einer Datei (F) von einer zweiten Rechnereinrichtung (200), die nicht zu einer sicheren Übertragung von Dateien eingerichtet ist, an eine erste Rechnereinrichtung (100), die zu einer sicheren Übertragung von Dateien eingerichtet ist, über eine cloudbasierte Plattform (P), mit den folgenden Schritten auf der zweiten Rechnereinrichtung (200):
- Ausführen einer von der ersten Rechnereinrichtung (100) bereitgestellten Verknüpfungsadresse (L) und Herstellen einer Verbindung mit der cloudbasierten Plattform (P),
- Auswählen einer zu übermittelnden Datei (F),
- Empfangen eines der ersten Rechnereinrichtung (100) zugeordneten öffentlichen Schlüssels (AK1) von der cloudbasierten Plattform (P),
- Generieren eines symmetrischen Dateischlüssels (SK),
- symmetrisches Verschlüsseln (A) der zu übermittelnden Datei (F) mit dem zufällig generierten Dateischlüssel (SK),
- asymmetrisches Verschlüsseln (B) des zufällig generierten Dateischlüssels (SK) mit dem empfangenen öffentlichen Schlüssel (AK1),
- Übermitteln,
- Hochladen der symmetrisch verschlüsselten Datei (Fx) auf mindestens einem cloudbasierten Speicher (S1, S2, S3),
- Übermitteln des asymmetrisch verschlüsselten symmetrischen Dateischlüssels (SK) an eine der cloudbasierten Plattform (P) zugeordnete Speichereinrichtung (M).

10. Verfahren nach Anspruch 9, das nach dem Schritt des Ausführens den zusätzlichen Schritt der Eingabe eines von der ersten Rechnereinrichtung (100) übermittelten Kennworts (PW) umfasst.

11. Verfahren nach einem der voranstehenden Ansprüche, mit dem zusätzlichen Schritt des Fragmentierens der verschlüsselten Datei (Fx) vor dem Schritt des Abspeicherns.

12. Computerprogramm mit Programmcodemitteln, um alle Schritte eines Verfahrens nach einem der Ansprüche 1 bis 11 durchzuführen, wenn das Computerprogramm auf einer Rechnereinrichtung (100, 200) und/oder einem Zentralserver (150) ausgeführt wird.

13. Computer (100, 150, 200), der zur Ausführung eines Verfahrens nach einem der Ansprüche 1 bis 11 eingerichtet ist.

Es folgen 8 Seiten Zeichnungen

Anhängende Zeichnungen

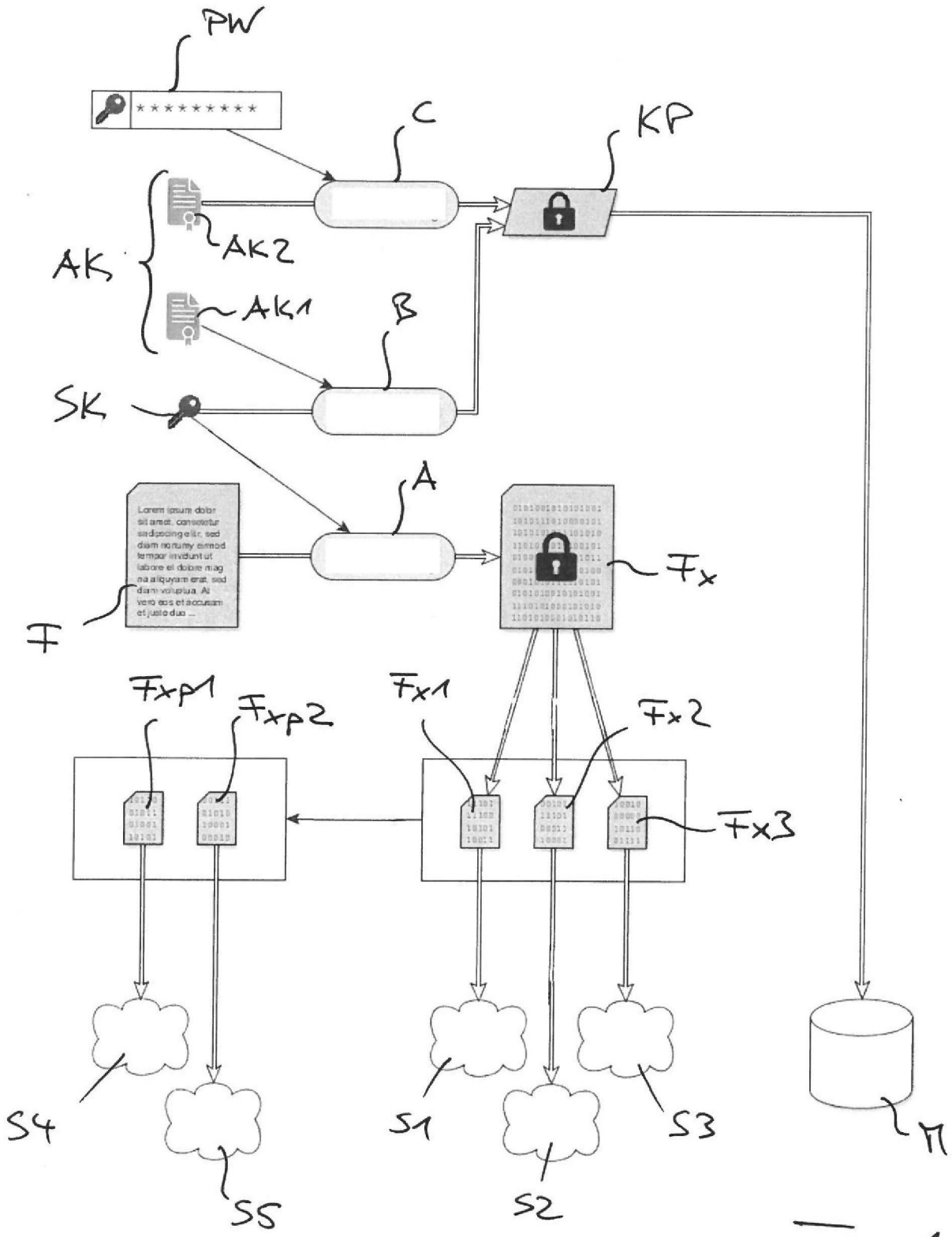


Fig. 1

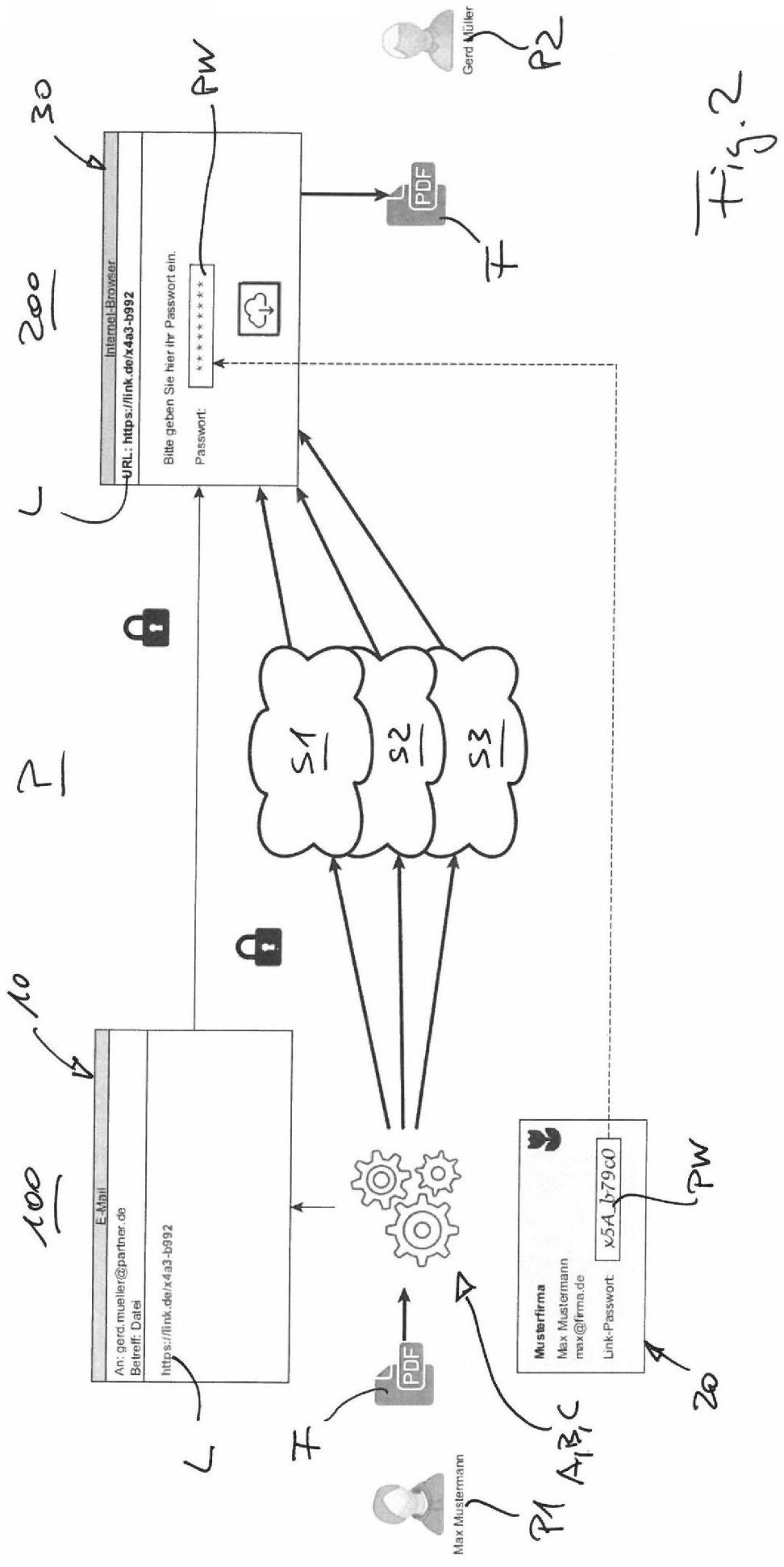

Gerd Müller
R2
PW
30
200
Internet-Browser
URL: https://link.de/x4a3-b992
Bitte geben Sie hier ihr Passwort ein.
Password:
****
PDF
T
L
21
S1
S2
S3
10
100
E-Mail
An: gerd.mueller@partner.de
Betreff: Datei
https://link.de/x4a3-b992
Musterfirma
Max Mustermann
max@firma.de
Link-Passwort:
x5A_b79c0
PW
20
L
T
PDF
A, B, C
Max Mustermann
P1

Fig. 2

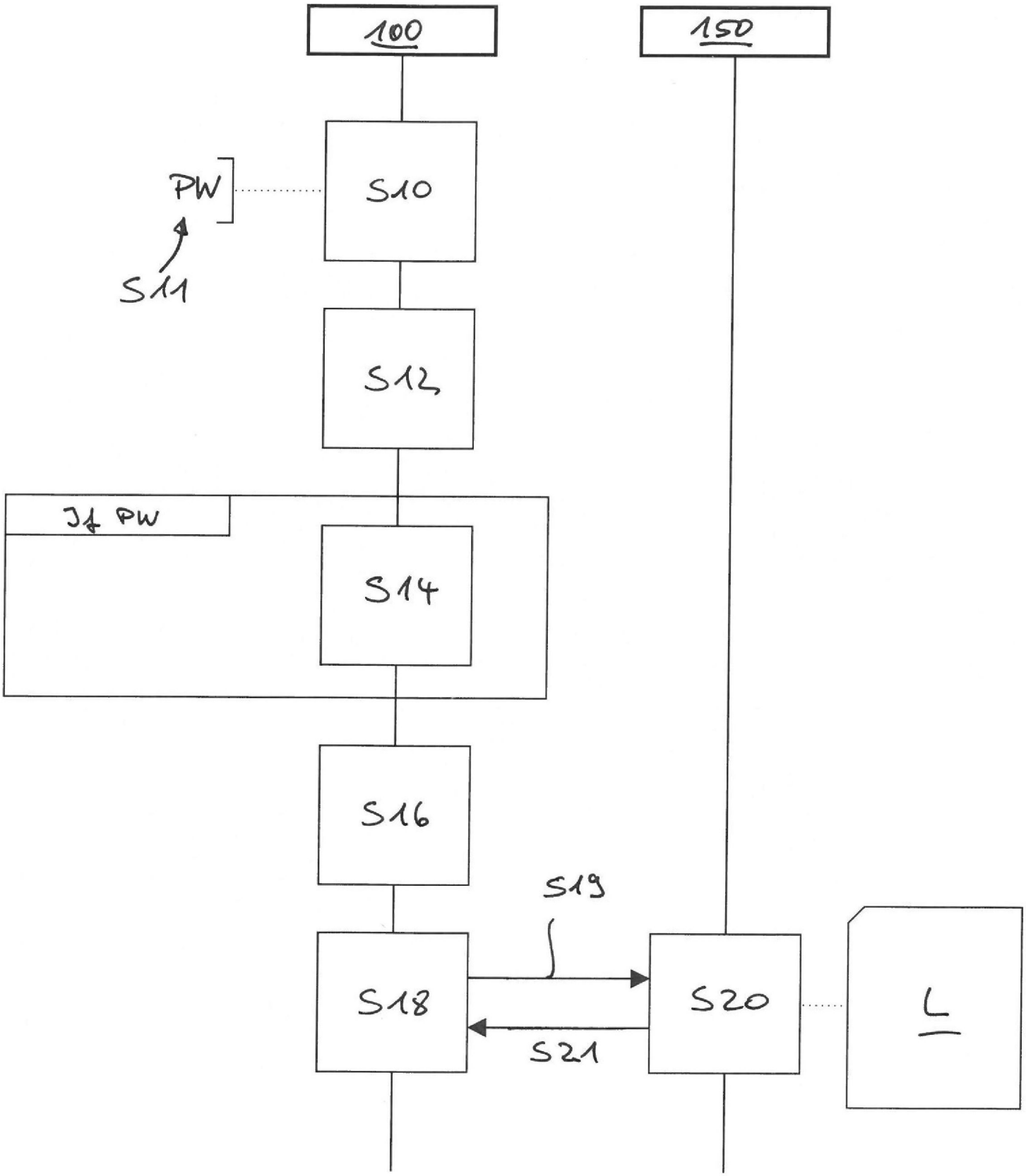
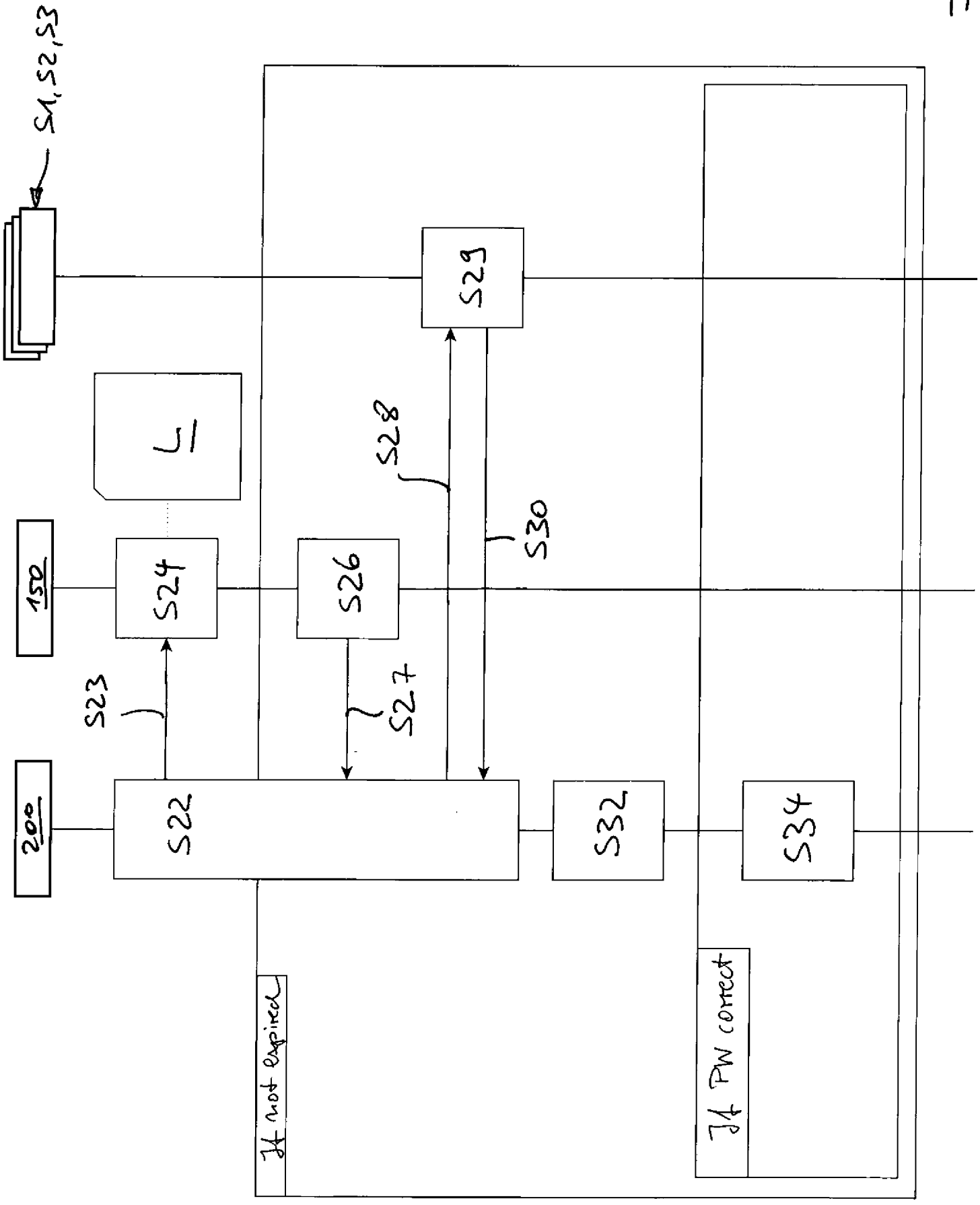


Fig. 3

Fig. 1


S1, S2, S3
S29
L1
S28
S30
150
S24
S26
S23
S27
200
S22
S32
S34
If not expired
If PW correct

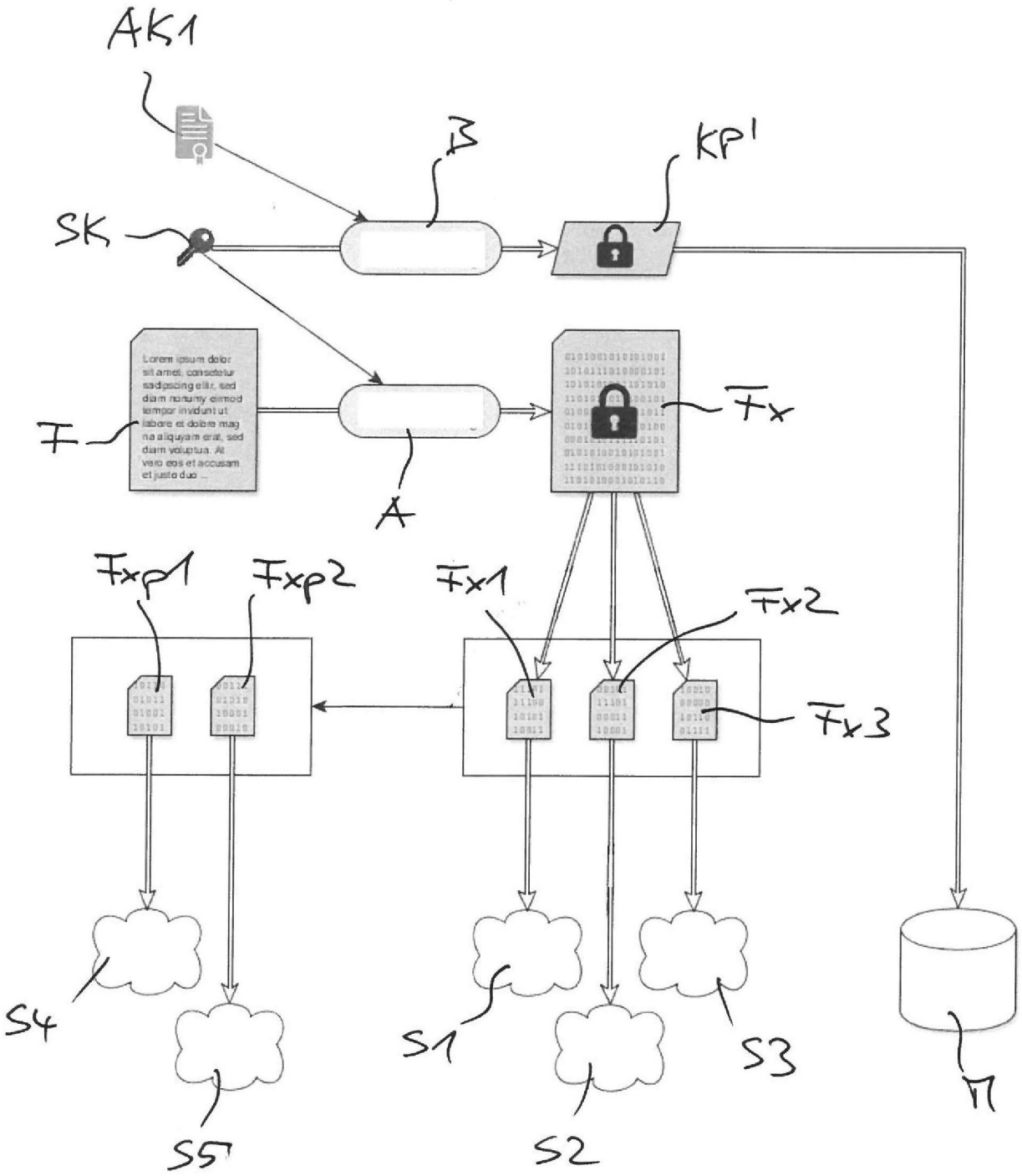


Fig. 5

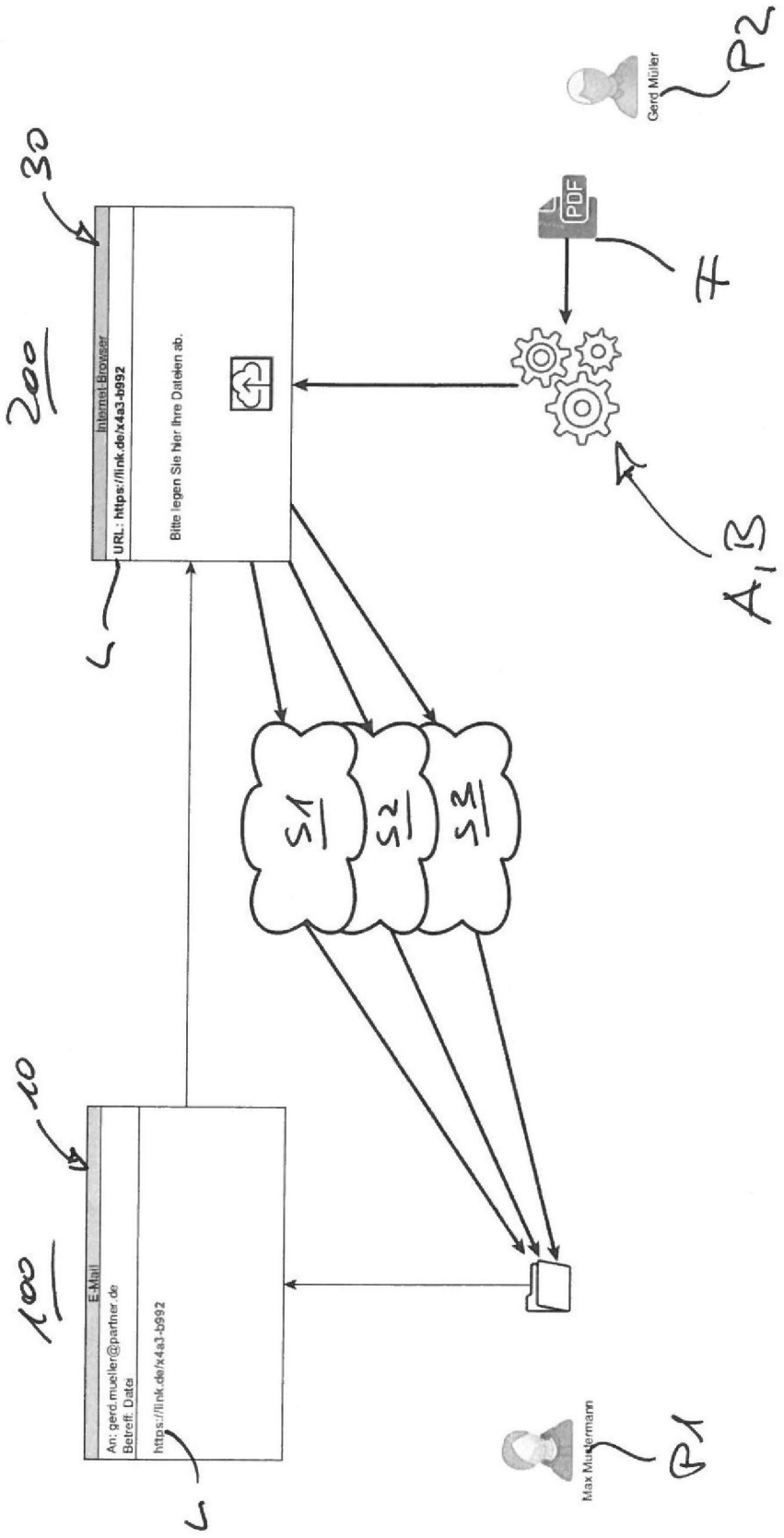

E-Mail
An: gerd.mueller@partner.de
Betreff: Data
https://link.de/x4a3-b992
Internet-Browser
URL: https://link.de/x4a3-b992
Bitte legen Sie hier Ihre Dateien ab.
PDF
Max Mustermann
Gerd Müller
100
10
200
30
P1
P2
H
A, B
S1
S2
SM

Fig. 6

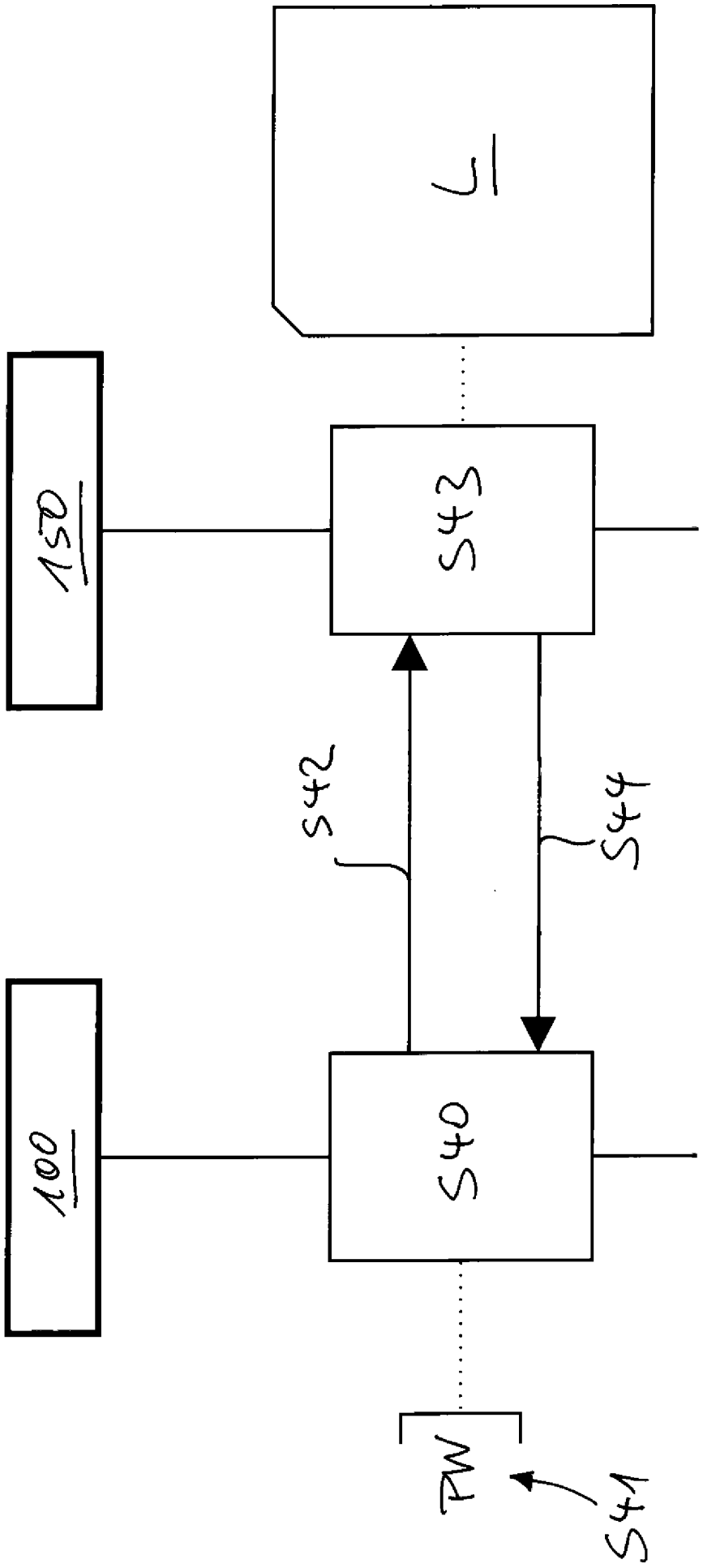


Fig. 7

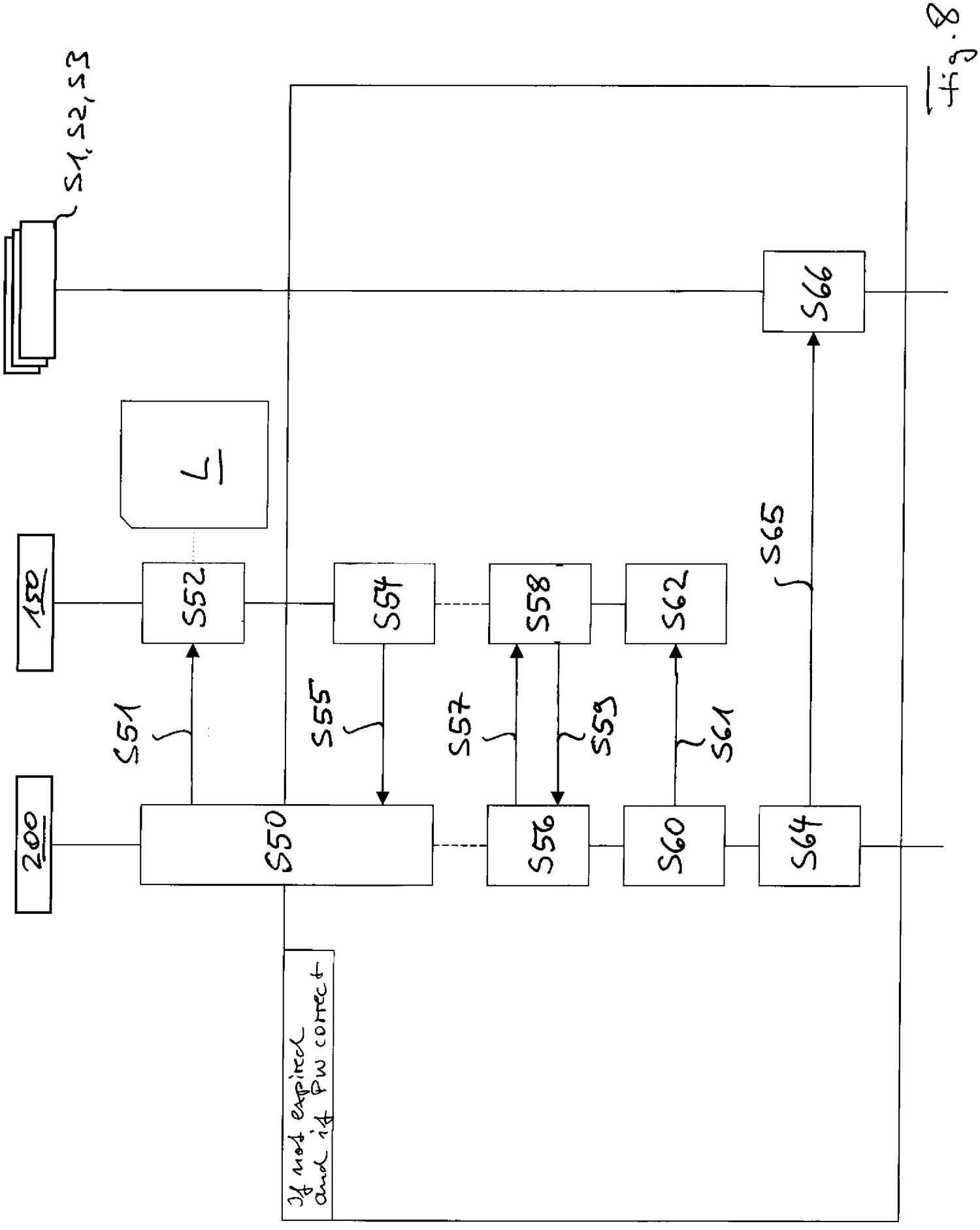


Fig. 8

