(19) österreichisches patentamt

(10) **AT 14348 U2 2015-09-15**

(12) # Gebrauchsmusterschrift

(21) Anmeldenummer: GM 87/2015
(22) Anmeldetag: 02.07.2013
(24) Beginn der Schutzdauer: 15.07.2015
(45) Veröffentlicht am: 15.09.2015

(51) Int. Cl.: ***G06F 21/64*** (2013.01)
G06Q 10/10 (2012.01)
H04L 9/32 (2006.01)

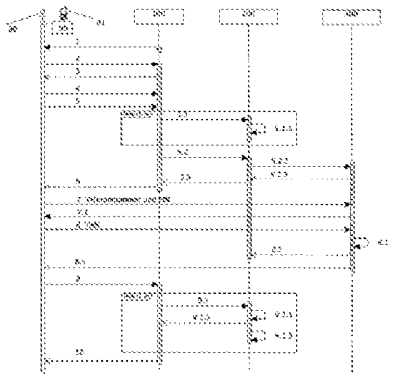
(60) Abzweigung aus A 552/2013

(73) Gebrauchsmusterinhaber:
XiTrust Secure Technologies GmbH
8010 Graz (AT)

(74) Vertreter:
Krassnigg Harald Dr.
8010 Graz (AT)

(54) **Verfahren und System zur Erzeugung einer elektronischen Stapelsignatur**

(57) Die Erfindung betrifft ein Verfahren zur Erzeugung einer elektronischen Stapelsignatur über mehrere zu signierende elektronische Dokumente. Die auf einer Signaturplattform (100) gespeicherten Dokumente werden nach Auswahl durch einen Signatur-Ersteller (80) an einen Signatur-Client (200) übermittelt, welcher eine Prüfsumme (5.1.1) für jedes Dokument erstellt. Die Prüfsummen werden an einen Signatur-Server (300) übermittelt, die Signaturplattform (100) übermittelt eine Signatur-Server-Adresse zur Eingabe von Identifikationsdaten (TelNr, PIN) an die Eingabe Vorrichtung (90). Anschließend erfolgt das Erstellen einer Verbindung (7.) durch die Eingabevorrichtung (90) mit dem Signatur-Server (300) und das Übermitteln (7.1) einer Transaktionsnummer (TAN) durch den Signatur-Server (300) an ein durch die Identifikationsdaten (TelNr, PIN) identifiziertes Endgerät (91), die Eingabe der Transaktionsnummer TAN (8.) durch den Signatur-Ersteller (80), die Berechnung einer Signatur für jede Prüfsumme durch den Signatur-Server (8.1), eine Übermittlung der Signaturen, eine Integration der Signaturen in die Dokumente durch den Signatur-Client (9.1.1), und eine Übertragung (9.1.2) der signierten Dokumente von dem Signatur-Client (200) an die Signaturplattform (100).



AT 14348 U2 2015-09-15

Beschreibung

VERFAHREN UND SYSTEM ZUR ERZEUGUNG EINER ELEKTRONISCHEN STAPELSIGNATUR

[0001] Die Erfindung betrifft ein Verfahren zur Erzeugung einer elektronischen Stapelsignatur über zwei oder mehrere zu signierende elektronische Dokumente.

[0002] Weiters betrifft die Erfindung ein System zum Durchführen eines oben genannten Verfahrens, umfassend eine Signaturplattform, einen Signatur-Client und einen mit der Signaturplattform und dem Signatur-Client zur Datenkommunikation verbundenen oder verbindbaren Signatur-Server.

[0003] Üblicherweise ist es zur rechtsgültigen Unterzeichnung eines Dokumentes notwendig, dass der Unterzeichner dieses Dokument eigenhändig auf Papier unterschreibt. Häufig liegen allerdings Dokumente nur noch in Form eines elektronischen Dokumentes, in der Regel als PDF-File vor. Im Zusammenhang mit dem sogenannten „papierlosen" Büro ist es häufig wünschenswert, auf Ausdrucke dieser Dokumente und eine Archivierung dieses physischen Dokumente verzichten zu können.

[0004] Es ist möglich, Dokumente in elektronischer Form zu signieren, beispielsweise kann eine rechtsgültige Signierung solcher elektronischen Dokumente mit einer sogenannten „Handysignatur" erfolgen.

[0005] Häufig sieht sich dabei ein Unterzeichner in der Situation, dass er mehrere Dokumente zu unterzeichnen hat. Es ist daher für einen Unterzeichner wünschenswert, diese rasch und mit geringem Aufwand rechtsgültig unterzeichnen zu können.

[0006] Es ist eine Aufgabe der Erfindung, ein Verfahren und ein System anzugeben, mit welchem für zwei oder mehrere elektronische Dokumente eine Stapelsignatur erzeugt werden kann, d.h., diese elektronischen Dokumente in einem Arbeitsgang durch den Unterzeichner rechtsgültig unterzeichnet werden können.

[0007] Diese Aufgabe wird mit einem eingangs erwähnten Verfahren erfindungsgemäß wie folgt gelöst:

[0008] a) Auswahlen der zu signierenden Dokumente, welche auf einer Signaturplattform gespeichert sind, mittels einer Eingabevorrichtung durch einen Signatur-Ersteller;

[0009] b) Übermitteln der ausgewählten Dokumente von der Signaturplattform an einen Signatur- Client;

[0010] c) Berechnen von jeweils einer Prüfsumme für jedes zu signierende Dokument durch den Signatur-Client;

[0011] d) Übermittlung der Prüfsummen aus Schritt c) durch den Signatur-Client an einen Signatur- Server;

[0012] e) Übermittlung einer Signatur-Server-Adresse zur Eingabe von Identifikationsdaten durch den Signatur-Ersteller zunächst vom Signatur-Server an den Signatur-Client, in weiterer Folge vom Signatur-Client an die Signaturplattform und schließlich von der Signaturplattform an die Eingabevorrichtung;

[0013] f) Erstellen einer Verbindung durch die Eingabevorrichtung mit dem Signatur-Server mittels der in Schritt e) übermittelten Signatur-Server-Adresse und Authentisierung des Signatur- Erstellers gegenüber dem Signatur-Server durch Eingabe von Identifikationsdaten;

[0014] g) Übermitteln einer Transaktionsnummer durch den Signatur-Server an ein durch die Identifikationsdaten identifiziertes Endgerät des Signatur-Erstellers;

[0015] h) Eingabe der Transaktionsnummer TAN durch den Signatur-Ersteller mittels der mit der Signatur-Server-Adresse verbundenen Eingabevorrichtung;

[0016] i) Berechnung einer Signatur für jede Prüfsumme durch den Signatur-Server nach korrekter Eingabe des „Freigabecodes";

[0017] j) Übermittlung der Signaturen, d.h. der signierten Prüfsummen durch den Signatur-Server an den Signatur-Client;

[0018] k) Integration der Signaturen in die zugehörigen Dokumente durch den Signatur-Client;

[0019] l) Übertragung der mit der Signatur unterschriebenen Dokumente von dem Signatur-Client an die Signaturplattform.

[0020] Weiters wird die Erfindung mit einem System umfassend eine Signaturplattform, einen Signatur-Client und einen Signatur-Server gelöst, wobei die Signaturplattform über den Signatur-Client mit dem Signatur-Server zur Datenkommunikation verbunden oder verbindbar ist, wobei die einzelnen Komponenten (Signaturplattform, Signatur-Client, Signatur-Server) zum Durchführen der jeweiligen Schritte des oben genannten Verfahrens eingerichtet sind.

[0021] Während die Signaturplattform, welche beispielsweise in einer Organisation, etwa einem Unternehmen, die Software-Infrastruktur für eine Signierung der Dokumente bietet, in das Netzwerk dieser Organisation integriert ist, befindet sich der Signatur-Server außerhalb der Einflusssphäre dieser Organisation. Der Signatur-Server befindet sich üblicherweise im Einflussbereich einer zertifizierten Stelle, etwa der Firma „A-Trust".

[0022] Durch die Verwendung eines Signatur-Clients, d.h. einer Software, welche Prüfsummen erstellt und mit dem Signatur-Server kommuniziert und dabei unter anderem die Prüfsummen an diesen übermittelt und die signierten Prüfsummen wieder entgegen nimmt, ist es nicht notwendig, dass die eigentlich zu signierenden Dokumente den Einflussbereich der Organisation, in welcher die Dokumente elektronisch vorliegen, verlässt, sodass sich dahingehend keine Probleme hinsichtlich Datensicherheit, Vertraulichkeit etc. ergeben können.

[0023] Im Folgenden ist die Erfindung an Hand der Zeichnung näher erläutert. In dieser zeigt die einzige Figur ein System zum Durchführen eines erfindungsgemäßen Verfahrens sowie das erfindungsgemäße Verfahren.

[0024] Die einzige Figur zeigt ein erfindungsgemäßes System bestehend aus einer Signaturplattform 100, einem Signatur-Client 200 und einem Signatur-Server 300.

[0025] Die Signaturplattform 100 ist eine Software, die auf einem Serversystem (der einsetzenden Organisation bzw. des einsetzenden Unternehmens) läuft. Sie bietet Schnittstellen für Menschen (Web-GUI für Auftraggeber und Unterschreiber) und Maschinen (Webservice-Schnittstelle zur Signaturplattform 100 zur Anlieferung und zur Abfrage von Signaturaufträgen).

[0026] Bei dem Signatur-Client 200 (im Folgenden auch Handysignatur-Client genannt) handelt es sich um einen lokal beim einsetzenden Kundenunternehmen/Organisation laufenden Teil der Signatur- bzw. Handysignatur-Gesamtanwendung (diese besteht aus dem Client 200 und dem Server 300). Aufgabe des Handysignatur-Clients 200 ist es, als Bindeglied zwischen der Signaturplattform 100 und dem Handysignatur-Server 300 zu fungieren. Seine Hauptaufgabe ist es, für ein zu signierendes Dokument, insbesondere PDF-Dokument eine Prüfsumme, vorzugsweise einen Hashwert zu berechnen, diesen an den Handysignatur- Server 300 zu senden, von diesem die Hashwert-Unterschrift wieder abzuholen und in das zu signierende Dokument, insbesondere PDF-Dokument zu integrieren. Durch dieses Verfahren wird vermieden, dass die Signaturplattform 100 das gesamte zu signierende Dokument, insbesondere PDF-Dokument zum Handysignatur-Server 300 schicken muss, welcher ja nicht in der einsetzenden Organisation bzw. dem einsetzenden Unternehmen steht, sondern bei einem Serviceprovider der Handysignatur.

[0027] Ein Benutzer bzw. Unterzeichner 80 kann sich mittels einer Eingabevorrichtung 90 mit der Signaturplattform 100 verbinden. Die Eingabevorrichtung 90 ist vorzugsweise ein Web-

Browser, welcher z.B. auf einem Personal-Computer läuft. Durch Eingabe einer entsprechenden Adresse in die Eingabevorrichtung 90 und anschließender Eingabe von Benutzername und Passwort kann sich der Benutzer 80 an der Signaturplattform 100 (an deren Web-GUI) anmelden und auf die ihm zugänglichen Daten und Dokumente zugreifen.

[0028] Weiters verfügt der Benutzer über ein vorzugsweise mobiles Endgerät 91, dessen Funktion im weiteren noch erläutert wird. Bei dem mobilen Endgerät handelt es sich beispielsweise um ein Mobilfunkgerät, beispielsweise um ein Smartphone oder einen Tablet-Computer, welches dem Benutzer über eine eindeutige Adresse, beispielsweise eine e-mail Adresse, vorzugsweise aber über eine Mobilfunknummer zugeordnet sind.

[0029] Derzeit gesteht der österreichische Gesetzgeber der Handysignatur nur dann den Charakter einer qualifizierten Signatur und damit die Rechtswirkung einer eigenhändigen Unterschrift zu, wenn die Authentisierung über eine SMS auf ein Mobiltelefon geschieht (Forderung des Gesetzgebers nach einer Zwei-Faktor-Authentisierung: eindeutige Zuordnung der Mobiltelefonnummer zu einem Benutzer, Eingabe eines PIN, den der Benutzer kennt).

[0030] Die eindeutige Zuordnung des Benutzers zu einer E-Mail-Adresse ist aus heutiger Sicht nicht in ausreichender Qualität machbar.

[0031] Falls dies in Zukunft möglich sein sollte, kann das erfindungsgemäße Verfahren aber auch z.B. unter Verwendung einer e-mail Adresse ausgeführt werden.

[0032] Die Eingabevorrichtung 90, d.h. in der Regel ein Web-Browser, kann grundsätzlich auch auf dem mobilen Endgerät 91 des Benutzers 80 laufen, wenn dieses dazu geeignet ist.

[0033] Im Folgenden sind an Hand der Figur die einzelnen Schritte des erfindungsgemäßen Verfahrens an Hand eines Beispiels näher erläutert.

SCHRITT 1

[0034] In Schritt 1 wird der Unterschreiber von der Signaturplattform 100 - nachdem sich der Benutzer wie oben beschrieben angemeldet hat - vom Vorhandensein eines oder mehrerer Signaturaufträge, also dem Vorliegen von zu unterzeichnenden Dokumenten benachrichtigt.

SCHRITT 2 UND SCHRITT 3

[0035] Der Unterschreiber 80 ruft daraufhin in Schritt 2 über seinen Webbrowser seine Unterschriftenmappe auf der Signaturplattform 100 auf und erhält somit eine Übersichtsdarstellung über alle von ihm zu unterschreibenden Aufträge (Schritt 3). Ein solcher Auftrag besteht im Wesentlichen aus einem PDF-Dokument und beschreibenden Informationen zu diesem PDF-Dokument.

SCHRITT 4

[0036] In Schritt 4 wählt der Unterschreiber 80 aus seiner Unterschriftenmappe jene Aufträge aus, die er im Stapelverfahren unterschreiben möchte (z.B. durch Anhaken einer Checkbox für jeden Auftrag).

SCHRITT 5

[0037] In Schritt 5 löst der Benutzer 80 dann den Unterschriftsprozess aus, in dem er einen entsprechenden Funktionsknopf in seiner Unterschriftenmappe drückt.

[0038] Die Signaturplattform 100 sendet daraufhin in Schritt 5.1 alle ausgewählten Auftragsdokumente an den Handysignatur-Client 200.

[0039] Der Handysignatur-Client 200 befindet sich dabei wie oben schon erwähnt in der selben Netzwerk-Sphäre wie die Signaturplattform 100, d.h. in der Regel in der internen IT (Intranet) jenes Unternehmens bzw. jener Organisation, das bzw. welche die Signaturplattform 100 einsetzt; damit ist gewährleistet, dass die Auftragsdokumente mit potentiell sensiblem Inhalt das

Unternehmen nicht verlassen.

[0040] In Schritt 5.1.1 berechnet der Handysignatur-Client 200 für jedes Auftragsdokument eine Prüfsumme vorzugsweise in Form eines Hash-Wertes, die dieses Dokument eindeutig repräsentiert.

[0041] In Schritt 5.2 signalisiert die Signaturplattform 100 dem Handysignatur-Client 200 den Abschluss der Stapelsignatur.

[0042] Dabei findet in Schritt 5.1 eine synchrone Kommunikation zwischen der Signaturplattform 100 und dem Handysignatur-Client 200 statt, d.h. die Signaturplattform 100 sendet die Anfrage mit dem Auftragsdokument an den Handysignatur-Client, dieser berechnet die Prüfsumme und meldet dies („bin fertig") dann als Antwort auf die Anfrage an die Signaturplattform 100.

[0043] Wenn die Signaturplattform 100 diese Antwort erhalten hat, wiederholt es entweder Schritt 5.1 mit einem weiteren Auftragsdokument, oder signalisiert in Schritt 5.2, dass (derzeit) keine weiteren Auftragsdokumente mehr kommen werden.

[0044] In weiterer Folge sendet, wenn keine weitere Auftragsdokumente mehr zum Unterzeichnen anstehen, der Handysignatur-Client 200 in Schritt 5.2.1 die Prüfsummen zum Handysignatur-Server 300, der sich wie schon beschrieben in einer anderen Netzwerk- Sphäre, beispielsweise im Rechenzentrum des Anbieters der Handysignatur befindet.

[0045] Der Handysignatur-Server 300 antwortet dem Signatur-Client 200 in Schritt 5.2.2 mit einer Adresse, vorzugsweise einer URL, für die Authentisierung des Benutzers mittels Telefonnummer und PIN; der Signatur-Client 200 antwortet daraufhin in weiterer Folge in Schritt 5.3 der Signaturplattform mit ebendieser Adresse.

SCHRITT 6

[0046] Diese Adresse wird dann von der Signaturplattform 100 an den Webbrowser des Unterschreibers 80 beispielsweise als HTTP Redirect weitergeben.

SCHRITT 7

[0047] Über diese Adresse verbindet sich der Webbrowser, also die Eingabevorrichtung 90 des Unterschreibers 80 in Schritt 7 mit dem Handysignatur-Server 300; dort gibt der Unterschreiber zur Authentisierung der Unterschriftsauslösung seine Telefonnummer und seinen PIN ein.

[0048] In Schritt 7.1 sendet der Handysignatur-Server 300 daraufhin auf das Endgerät 91 des Unterschreibers 80 eine einmal gültige Transaktionsnummer TAN.

SCHRITT 8

[0049] Der Unterschreiber 80 gibt dann auf der Webseite des Handysignatur-Servers 300 die erhaltene Transaktionsnummer TAN ein, um die Auslösung der Signaturen am Signatur-Server 300 zu autorisieren.

[0050] In Schritt 8.1 berechnet der Handysignatur-Server 300 nun eine Signatur für jede Prüfsumme, und sendet diese Signaturen in Schritt 8.2 an den Handysignatur-Client 200 zurück.

[0051] In Schritt 7.3 leitet der Handysignatur-Server 300 den Unterschreiber per HTTP Redirect zur Ergebnisseite der Stapelsignatur-Operation auf die Signaturplattform 100 zurück.

SCHRITT 9

[0052] Der Webbrowser 90 des Unterschreibers 80 verbindet sich nun in Schritt 9 mit dieser Ergebnisseite, wo nun eine aktualisierte Darstellung seiner Unterschriftenmappe ausgegeben wird.

[0053] Um diese aktualisierte Darstellung der Unterschriftenmappe darstellen zu können, ruft

die Signaturplattform 100 in Schritt 9.1 alle unterschriebenen Auftragsdokumente vom Handysignatur-Client 200 ab. Dieser integriert daraufhin in Schritt 9.1.1 die in Schritt 8.2 vom Handysignatur-Server 300 erhaltenen Signaturen in die Auftragsdokumente und sendet die signierten Auftragsdokumente in Schritt 9.1.2 zurück an die Signaturplattform 100. Abschließend löscht der Handysignatur-Client in Schritt 9.1.3 die Auftragsdokumente, da sie in seiner Sphäre nicht mehr weiter benötigt werden (wiederum eine Maßnahme, um die potentiell sensiblen Inhalte der Auftragsdokumente zu schützen).

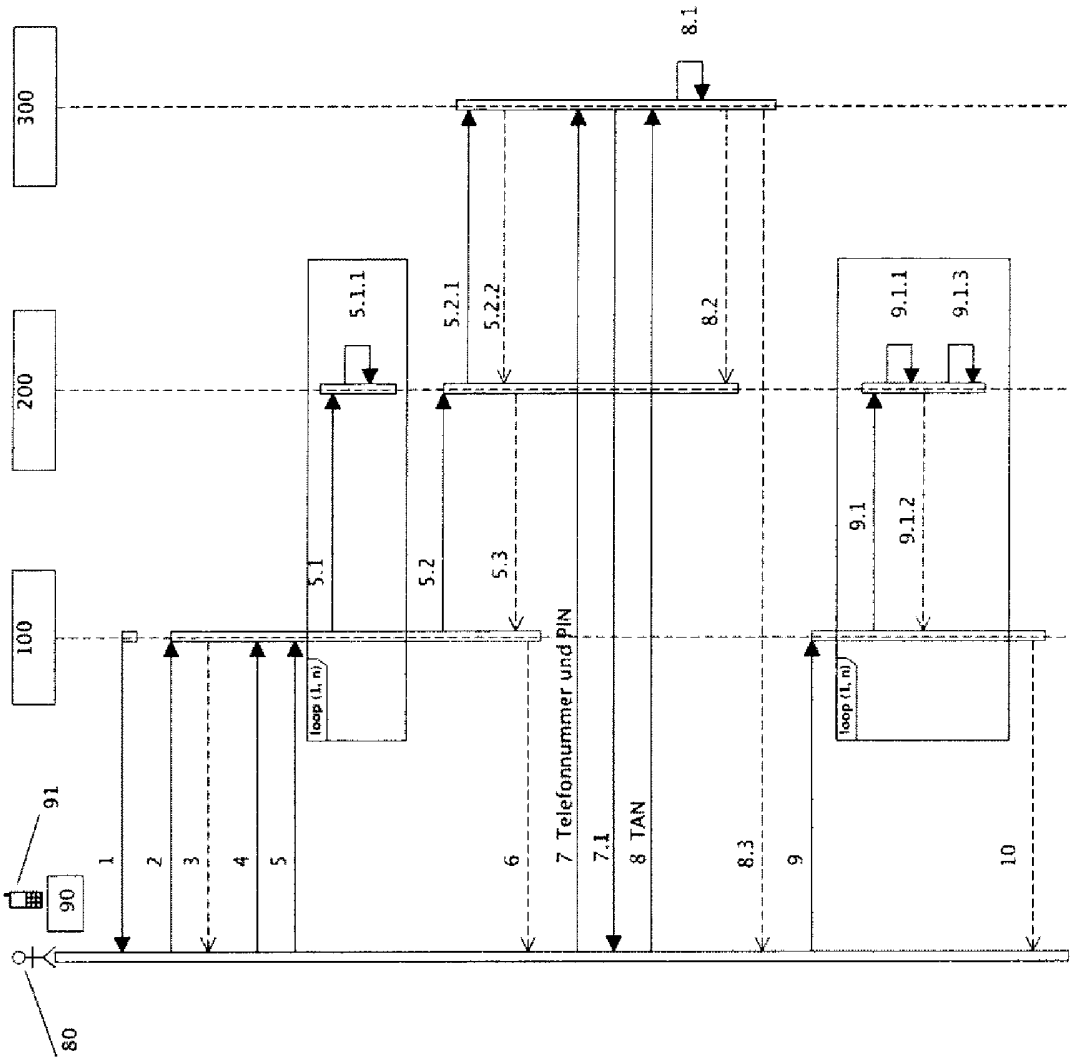
SCHRITT 10

[0054] In Schritt 10 schließlich erhält der Unterschreiber in seinem Webbrowser die aktualisierte Darstellung seiner Unterschriftenmappe, in der nun alle von ihm in Schritt 4 ausgewählten Auftragsdokumente mit seiner Unterschrift versehen sind.

Ansprüche

1. Verfahren zur Erzeugung einer elektronischen Stapelsignatur über zwei oder mehrere zu signierende elektronische Dokumente, **gekennzeichnet durch** die folgenden Schritte:
   a) Auswählen der zu signierenden Dokumente, welche auf einer Signaturplattform (100) gespeichert sind (4.), mittels einer Eingabevorrichtung (90) durch einen Signatur-Ersteller (80);
   b) Übermitteln der ausgewählten Dokumente (5.1) von der Signaturplattform (100) an einen Signatur-Client (200);
   c) Berechnen von jeweils einer Prüfsumme (5.1.1) für jedes zu signierende Dokument durch den Signatur-Client (200);
   d) Übermittlung (5.2.1) der Prüfsummen aus Schritt c) durch den Signatur-Client (200) an einen Signatur-Server (300);
   e) Übermittlung (5.2.2, 5.3, 6) einer Signatur-Server-Adresse zur Eingabe von Identifikationsdaten (TelNr, PIN) durch den Signatur-Ersteller (80) zunächst vom Signatur-Server (300) an den Signatur-Client (200), in weiterer Folge vom Signatur-Client (200) an die Signaturplattform (100) und schließlich von der Signaturplattform (100) an die Eingabe-Vorrichtung (90);
   f) Erstellen einer Verbindung (7.) durch die Eingabevorrichtung (90) mit dem Signatur-Server (300) mittels der in Schritt e) übermittelten Signatur-Server-Adresse und Authentisierung des Signatur-Erstellers (80) gegenüber dem Signatur-Server (300) durch Eingabe von Identifikationsdaten (TelNr, PIN);
   g) Übermitteln (7.1) einer Transaktionsnummer (TAN) durch den Signatur-Server (300) an ein durch die Identifikationsdaten (TelNr, PIN) identifiziertes Endgerät (91) des Signatur-Erstellers (80);
   h) Eingabe der Transaktionsnummer TAN (8.) durch den Signatur-Ersteller (80) mittels der mit der Signatur-Server-Adresse verbundenen Eingabevorrichtung (90);
   i) Berechnung einer Signatur für jede Prüfsumme durch den Signatur-Server (8.1) nach korrekter Eingabe des „Freigabecodes" (PIN, TAN);
   j) Übermittlung der Signaturen, d.h. der signierten Prüfsummen durch den Signatur-Server (300) an den Signatur-Client (8.2);
   k) Integration der Signaturen in die zugehörigen Dokumente durch den Signatur-Client (9.1.1);
   l) Übertragung (9.1.2) der mit der Signatur unterschriebenen Dokumente von dem Signatur-Client (200) an die Signaturplattform (100).
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die Prüfsummen Hash-Werte sind.
3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass das Endgerät (91) des Benutzers ein Mobilfunkgerät, beispielsweise ein Smartphone ist.
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass sich der Signatur-Server (300) außerhalb der Netzwerk-Sphäre der Signaturplattform (100) befindet.
5. System zum Durchführen eines Verfahrens nach einem der Ansprüche 1 bis 4, umfassend eine Signaturplattform (100), einen Signatur-Client (200) und einen mit dem Signatur-Client (200) zur Datenkommunikation verbundenen oder verbindbaren Signatur- Server (300).
6. System nach Anspruch 5, **dadurch gekennzeichnet**, dass sich der Signatur-Server (300) außerhalb der Netzwerk-Sphäre der Signaturvorrichtung (100) befindet.

Hierzu 1 Blatt Zeichnungen


300
200
100
8.1
5.1.1
5.2.1
5.2.2
8.2
9.1.1
9.1.3
9.1
9.1.2
5.1
5.2
5.3
loop (1, n)
loop (1, n)
7 Telefonnummer und PIN
7.1
8 TAN
8.3
91
90
80
1
2
3
4
5
6
9
10