

(12) **Gebrauchsmusterschrift**

(21) Anmeldenummer: GM 8014/2018 (51) Int. Cl.: **G06F 21/64** (2013.01)  
 (22) Anmeldetag: 18.11.2015 **G06Q 10/10** (2012.01)  
 (24) Beginn der Schutzdauer: 15.12.2018 **H04L 9/32** (2006.01)  
 (45) Veröffentlicht am: 15.12.2018

(67) Umwandlung von A 743/2015

(56) Entgegenhaltungen:  
 AT 514544 A1  
 AT 14348 U2  
 Arnold A., "Alle TAN-Verfahren im Überblick".  
 [online]. PC-Welt > Computer & Technik >  
 Sicherheit > Antivirus & Firewall > Online-Banking,  
 29.09.2013 [ermittelt am 26.03.2018]. Ermittelt im  
 Internet <URL:  
[https://www.pcwelt.de/ratgeber/Alle\\_TAN-Verfahren\\_im\\_Ueberblick-Online-Banking-7966613.html](https://www.pcwelt.de/ratgeber/Alle_TAN-Verfahren_im_Ueberblick-Online-Banking-7966613.html)>

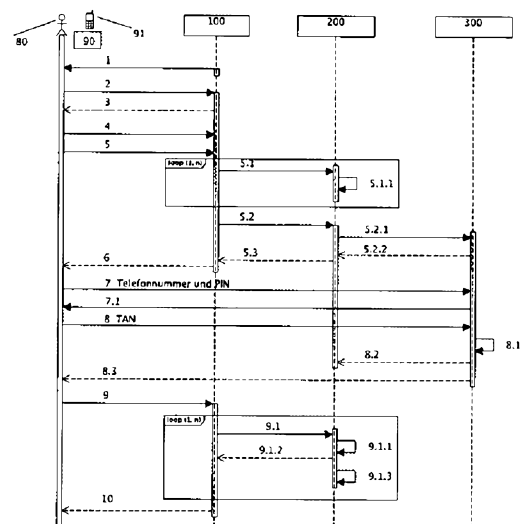
(73) Gebrauchsmusterinhaber:  
 XiTrust Secure Technologies GmbH  
 8010 Graz (AT)

(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 Eingabevorrichtung (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). Die Transaktionsnummer (TAN) wird von dem Signatur-Server (300) an eine auf dem Endgerät (91) laufende Signatur-App übermittelt, wobei diese Signatur-App mit einer Identifikationsinformation des Endgerätes (91) verknüpft ist.



## 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, welches Verfahren die folgenden, insbesondere der Reihe nach ausgeführten, Schritte umfasst:

- [0002]** a) Auswählen der zu signierenden Dokumente, welche auf einer Signaturplattform gespeichert sind, mittels einer Eingabevorrichtung durch einen Signatur-Ersteller;
- [0003]** b) Übermitteln der ausgewählten Dokumente von der Signaturplattform an einen Signatur-Client;
- [0004]** c) Berechnen von jeweils einer Prüfsumme für jedes zu signierende Dokument durch den Signatur-Client;
- [0005]** d) Übermittlung der Prüfsummen aus Schritt c) durch den Signatur-Client an einen Signatur-Server;
- [0006]** 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;
- [0007]** 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;
- [0008]** g) Übermitteln einer Transaktionsnummer durch den Signatur-Server an ein durch die Identifikationsdaten identifiziertes Endgerät des Signatur-Erstellers;
- [0009]** h) Eingabe der Transaktionsnummer TAN durch den Signatur-Ersteller mittels der mit der Signatur-Server-Adresse verbundenen Eingabevorrichtung;
- [0010]** i) Berechnung einer Signatur für jede Prüfsumme durch den Signatur-Server nach korrekter Eingabe des „Freigabecodes“, welcher Freigabecode insbesondere aus der Transaktionsnummer besteht,
- [0011]** j) Übermittlung der Signaturen, d.h. der signierten Prüfsummen durch den Signatur-Server an den Signatur-Client;
- [0012]** k) Integration der Signaturen in die zugehörigen Dokumente durch den Signatur-Client;
- [0013]** l) Übertragung der mit der Signatur unterschriebenen Dokumente von dem Signatur-Client an die Signaturplattform.

**[0014]** 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.

**[0015]** Ein oben beschriebenes Verfahren bzw. System ist aus der AT 514544 A1 und der AT 14348 U2 bekannt.

**[0016]** 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 dieser physischen Doku-

mente verzichten zu können.

**[0017]** Es ist möglich, Dokumente in elektronischer Form zu signieren, beispielsweise kann eine rechtsgültige Signierung solcher elektronischen Dokumente mit einer sogenannten „Handysignatur“ erfolgen.

**[0018]** 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.

**[0019]** Mit einem oben beschriebenen Verfahren bzw. System kann für zwei oder mehrere elektronische Dokumente eine Stapelsignatur erzeugt werden kann, d.h., diese elektronischen Dokumente können in einem Arbeitsgang durch den Unterzeichner rechtsgültig unterzeichnet werden.

**[0020]** 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 Einflussosphäre dieser Organisation. Der Signatur-Server befindet sich üblicherweise im Einflussbereich einer zertifizierten Stelle, etwa der Firma „A-Trust“.

**[0021]** 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.

**[0022]** Bei einem bekannten Verfahren werden als Identifikationsdaten eine Telefonnummer und ein PIN übermittelt, und die Transaktionsnummer, insbesondere ein TAN, wird als SMS an diese Telefonnummer übermittelt.

**[0023]** Es ist eine Aufgabe der Erfindung, die Sicherheit bekannter Verfahren zu erhöhen bzw. die Benutzbarkeit des Signatur-Verfahrens sicher zu stellen.

**[0024]** Diese Aufgabe wird mit einem eingangs erwähnten Verfahren dadurch gelöst, dass in Schritt g) die Transaktionsnummer von dem Signatur-Server an eine auf dem Endgerät laufende Signatur-App übermittelt wird, wobei diese Signatur-App mit einer Identifikationsinformation des Endgerätes, vorzugsweise einer dem Endgerät zugeordneten Telefonnummer/Rufnummer verknüpft ist.

**[0025]** Die Identifikationsinformationen des Endgerätes zur Verknüpfung mit der Signatur-App sind die Telefonnummer, oder optionale eine Kombination aus IMEI des Endgerätes und Telefonnummer.

**[0026]** 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.

**[0027]** Bei der Signatur-App handelt es sich um eine eigenständige Applikation, an welche die Transaktionsnummer TAN übermittelt wird (bei bestehender Internetverbindung). Der TAN erscheint daher nicht als Nachricht in einer SMS-App, sondern in dieser eigenständigen Signatur-App. Falls somit die Übermittlung der Transaktionsnummer per SMS unsicher wäre oder werden würde, so steht mit der Signatur-App ein zusätzlicher Kanal zur Verfügung, über den die Übermittlung der Transaktionsnummer anders funktioniert, wodurch der gesamte Signatur-Service an sich abgesichert wird, sodass die Signaturlösung weiterhin, auch bei unsicherer SMS, genutzt werden kann.

**[0028]** Die Erfindung stellt somit ein alternatives Verfahren bereit, sodass einerseits der Benut-

zer die Wahl hat, welches Verfahren für ihn bequemer oder in der Situation besser geeignet ist, und andererseits steht damit ein zweiter Kanal zur Verfügung, falls ein Kanal ausfallen sollte oder unsicher wird bzw. ist.

**[0029]** Im Folgenden ist die Erfindung an Hand der Zeichnung näher erläutert. In dieser zeigt die einzige Figur 1 ein System zum Durchführen eines erfindungsgemäßen Verfahrens sowie das erfindungsgemäße Verfahren.

**[0030]** Die einzige Figur 1 zeigt ein erfindungsgemäßes System bestehend aus einer Signaturplattform 100, einem Signatur-Client 200 und einem Signatur-Server 300.

**[0031]** 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).

**[0032]** 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.

**[0033]** 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.

**[0034]** 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.

**[0035]** Es kann die angesprochene Eingabevorrichtung 90 auch von dem mobile Endgerät 91 realisiert sein, beispielsweise indem die Eingabevorrichtung 90 ein Webbrowser ist, der auf dem mobilen Endgerät 91 des Benutzers 80 läuft. Allerdings wird in diesem Fall die üblicherweise gegebene Zwei-Faktor-Authentifizierung auf einen Faktor reduziert.

**[0036]** 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 Zwei-Faktor-Authentisierung erfolgt, was mittels einer eindeutigen Zuordnung der Mobiltelefonnummer zu einem Benutzer und Eingabe eines PIN, den der Benutzer kennt, erfolgen kann.

**[0037]** Die eindeutige Zuordnung des Benutzers zu einer E-Mail-Adresse ist aus heutiger Sicht nicht in ausreichender Qualität machbar.

**[0038]** Falls dies in Zukunft möglich sein sollte, kann das erfindungsgemäße Verfahren aber auch z.B. unter Verwendung einer e-mail Adresse ausgeführt werden.

**[0039]** Im Folgenden sind an Hand der Figur die einzelnen Schritte des erfindungsgemäßen

Verfahrens an Hand eines Beispiels näher erläutert.

#### SCHRITT 1

**[0040]** 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

**[0041]** 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

**[0042]** 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

**[0043]** In Schritt 5 löst der Benutzer 80 dann den Unterschriftenprozess aus, in dem er einen entsprechenden Funktionsknopf in seiner Unterschriftenmappe drückt.

**[0044]** Die Signaturplattform 100 sendet daraufhin in Schritt 5.1 alle ausgewählten Auftragsdokumente an den Handysignatur-Client 200.

**[0045]** Der Handysignatur-Client 200 befindet sich dabei wie oben schon erwähnt in derselben 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.

**[0046]** 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.

**[0047]** In Schritt 5.2 signalisiert die Signaturplattform 100 dem Handysignatur-Client 200 den Abschluss der Stapelsignatur.

**[0048]** Dabei findet in Schritt 5.1 vorzugsweise 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.

**[0049]** 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.

**[0050]** In weiterer Folge sendet, wenn keine weiteren Auftragsdokumente mehr zum Unterschreiben 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.

**[0051]** 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. Der Signatur-Client 200 antwortet daraufhin in weiterer Folge in Schritt 5.3 der Signaturplattform 100 mit

ebendieser Adresse.

#### SCHRITT 6

**[0052]** Diese Adresse, vorzugsweise URL, wird dann von der Signaturplattform 100 an den Webbrowser des Unterschreibers 80 beispielsweise als HTTP Redirect weitergeben.

#### SCHRITT 7

**[0053]** 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 Identifikationsdaten, insbesondere Telefonnummer und seinen PIN ein.

**[0054]** Unter dem „Eingeben“ der Telefonnummer ist dabei zu verstehen, dass diese dem Handysignatur-Server 300 angegeben werden muss. Entweder geschieht dies durch ein tatsächliches Eingeben durch den Benutzer im Browser, oder der Browser hat die Telefonnummer bereits gespeichert, wie dies bei modernen Browsern möglich ist.

**[0055]** Der PIN wird vorzugsweise immer manuell eingegeben und ist nicht im Browser gespeichert.

**[0056]** Bei dem PIN handelt es sich typischerweise um einen PIN-Code, z.B. einen Zahlencode, es kann sich dabei aber auch um ein beliebiges Passwort handeln, das allerdings hinsichtlich der notwendigen Sicherheit gewissen Anforderungen unterliegt.

**[0057]** Erfindungsgemäß erfolgt nun die Transaktionsfreigabe mittels einer eigens dafür vorgesehenen Signatur-App, die am mobilen Endgerät 91 des Benutzers ausgeführt wird. Bei einer sogenannten „App“ handelt es sich um eine Anwendungssoftware für Mobilgeräte oder mobile Betriebssysteme. Dazu ist es notwendig, dass diese Signatur-App initial einmal mit der Handysignatur des Benutzers gekoppelt wurde. Dies erfolgt mittels eines Registrierungsprozesses, bei dem die Telefonnummer des mobilen Endgerätes oder eine Kombination aus Telefonnummer und IMEI des Endgerätes mit dieser Signatur-App verknüpft wird.

**[0058]** Für diese Signatur-App wird nun, vorzugsweise am Handysignatur-Server 300, eine Transaktionsnummer TAN, die vorzugsweise nur einmal gültig ist, generiert. In Schritt 7.1 sendet der Handysignatur-Server 300 daraufhin an die Signatur-App auf dem Endgerät 91 des Unterschreibers 80 diese, insbesondere nur einmal gültige, Transaktionsnummer TAN.

**[0059]** Diese Transaktionsnummer TAN wird in der Signatur-App auf dem Endgerät 91 des Benutzers 80 angezeigt, und dieser kann die Transaktionsnummer TAN in einem nächsten Schritt eingeben, wie dies weiter unten in Schritt 8 beschrieben ist.

**[0060]** Bei einer konkreten Ausführungsform kann dabei vorgesehen sein, dass der Benutzer bei oder nach der Eingabe des Signaturpasswortes, vorzugsweise in Form eines PIN-Codes, die Art der Transaktionsfreigabe, nämlich wie vorstehend beschrieben mittels App oder alternativ mittels SMS („Short-Message-Service“), auswählen kann. In letzterem Fall muss allerdings, sofern diese nicht schon in Zusammenhang mit dem Signaturpasswort bereits hinterlegt ist, noch eine Telefonnummer des mobilen Endgerätes eingegeben werden, an welche dann die Transaktionsnummer mittels SMS übermittelt wird. Insgesamt muss der Benutzer nur einmal pro Transaktion die Rufnummer seines Endgerätes eingeben. An diese Telefonnummer aus dem Schritt, in dem er Telefonnummer und PIN eingibt, wird auch die Transaktionsnummer TAN geschickt, je nach Auswahl des Benutzers an die Signatur-App oder mittels SMS.

#### SCHRITT 8

**[0061]** Der Unterschreiber 80 gibt dann auf der Webseite des Handysignatur-Servers 300 seinen Freigabecode in Form der erhaltenen Transaktionsnummer TAN, welche in der Signatur-App angezeigt wird, ein, z.B. in einem dafür vorgesehenen Signaturfenster (beispielsweise in demselben Fenster, das auch angezeigt würde, wenn die TAN per SMS käme), um die Auslö-

sung der Signaturen am Signatur-Server 300 zu autorisieren.

**[0062]** Der Freigabecode ist die Transaktionsnummer TAN, die exakt an diese eine Transaktion gebunden ist. Mit Eingabe der TAN wird die Signatur ausgelöst, die TAN hat aber kein besonderes Schema, aus dem sie besteht.

**[0063]** 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.

**[0064]** In Schritt 8.3 leitet (stimmt so) der Handysignatur-Server 300 den Unterschreiber per HTTP Redirect zur Ergebnisseite der Stapelsignatur-Operation auf die Signaturplattform 100 zurück.

## SCHRITT 9

**[0065]** Der Webbrowser 90 des Unterschreibers 80 verbindet sich nun in Schritt 9 mit dieser Ergebnisseite, wo nun eine aktualisierte Darstellung seiner Unterschriftenmappe ausgegeben wird.

**[0066]** 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

**[0067]** 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, mit den folgenden Schritten:
  - 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 Eingabevorrichtung (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“ (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).

**dadurch gekennzeichnet**, dass

in Schritt g) die Transaktionsnummer (TAN) von dem Signatur-Server (300) an eine auf dem Endgerät (91) laufende Signatur-App übermittelt wird, wobei diese Signatur-App mit einer Identifikationsinformation des Endgerätes (91), vorzugsweise einer dem Endgerät (91) zugeordneten Telefonnummer/Rufnummer verknüpft ist.

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 Signaturplattform (100) befindet.

**Hierzu 1 Blatt Zeichnungen**

1/1

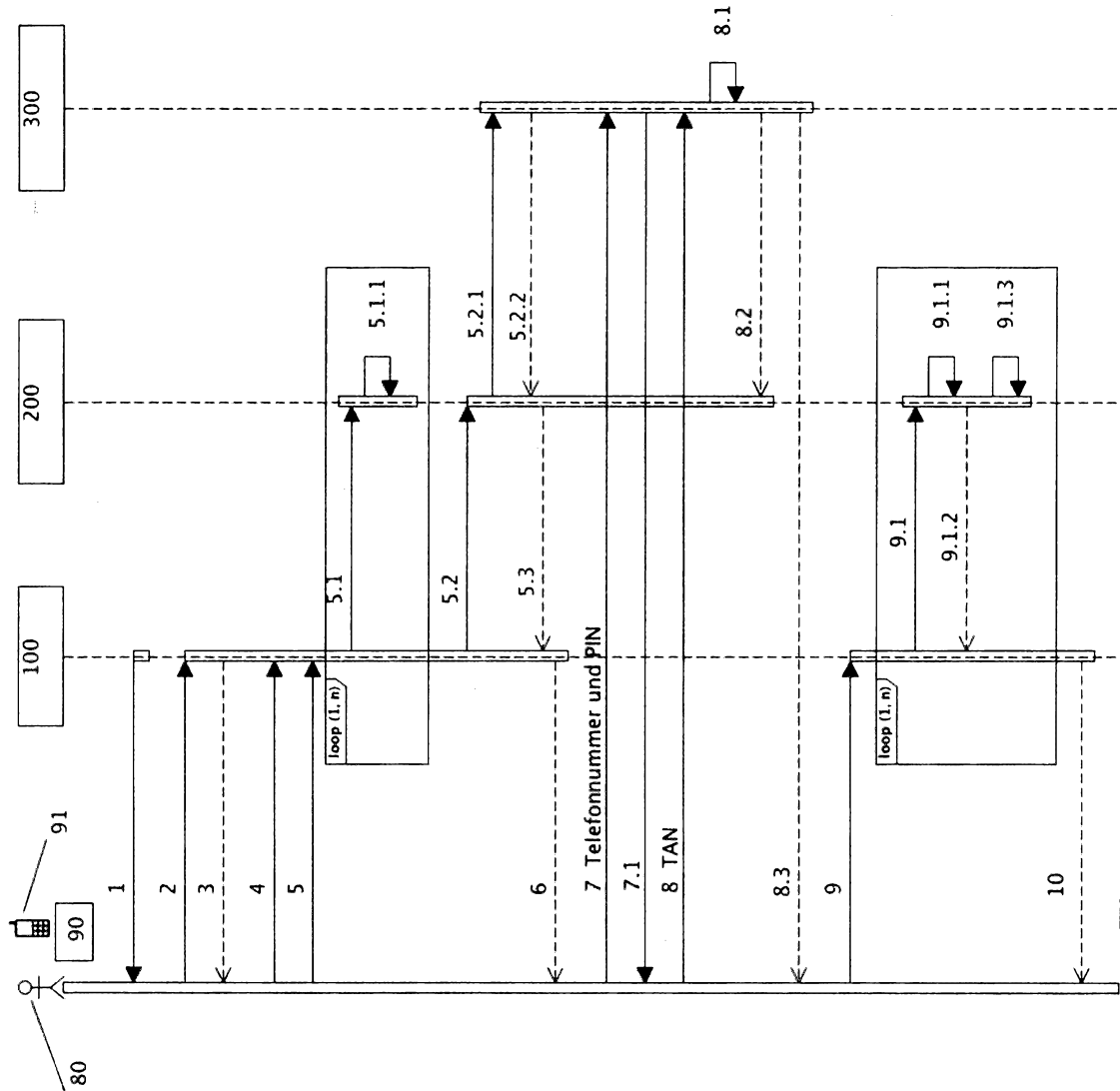


Fig. 1

Klassifikation des Anmeldungsgegenstands gemäß IPC:  
**G06F 21/64** (2013.01); **G06Q 10/10** (2012.01); **H04L 9/32** (2006.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:  
**G06F 21/645** (2013.01); **G06Q 10/10** (2018.01); **H04L 9/3247** (2013.01)

Recherchierter Prüfstoff (Klassifikation):  
 G06F, G06Q, H04L

Konsultierte Online-Datenbank:  
 EPODOC, WPI

Dieser Recherchenbericht wurde zu den am **24.07.2017** eingereichten Ansprüchen **1-6** erstellt.

Kategorie <sup>1)</sup>	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	AT 514544 A1 (XITRUST SECURE TECHNOLOGIES GMBH) 15. Januar 2015 (15.01.2015) gesamtes Dokument	1-6
X	AT 14348 U2 (XITRUST SECURE TECHNOLOGIES GMBH) 15. September 2015 (15.09.2015) gesamtes Dokument	1-6
A	Arnold A., "Alle TAN-Verfahren im Überblick". [online]. PC-Welt > Computer & Technik > Sicherheit > Antivirus & Firewall > Online-Banking, 29.09.2013 [ermittelt am 26.03.2018]. Ermittelt im Internet <URL: <a href="https://www.pcwelt.de/ratgeber/Alle_TAN-Verfahren_im_Ueberblick-Online-Banking-7966613.html">https://www.pcwelt.de/ratgeber/Alle_TAN-Verfahren_im_Ueberblick-Online-Banking-7966613.html</a> > gesamtes Dokument, insbesondere Abschnitt "pushTAN"	1-6

Datum der Beendigung der Recherche: 26.03.2018	Seite 1 von 1	Prüfer(in): PRAMHAS Atilla
---	---------------	-------------------------------

<sup>1)</sup> **Kategorien der angeführten Dokumente:**

<p><b>X</b> Veröffentlichung <b>von besonderer Bedeutung</b>: der Anmeldegegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.</p>	<p><b>A</b> Veröffentlichung, die den allgemeinen <b>Stand der Technik</b> definiert.</p>
<p><b>Y</b> Veröffentlichung <b>von Bedeutung</b>: der Anmeldegegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese <b>Verbindung für einen Fachmann naheliegend</b> ist.</p>	<p><b>P</b> Dokument, das <b>von Bedeutung</b> ist (Kategorien X oder Y), jedoch <b>nach dem Prioritätstag</b> der Anmeldung veröffentlicht wurde.</p> <p><b>E</b> Dokument, das <b>von besonderer Bedeutung</b> ist (Kategorie X), aus dem ein „<b>älteres Recht</b>“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).</p> <p><b>&amp;</b> Veröffentlichung, die Mitglied der selben <b>Patentfamilie</b> ist.</p>