(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. Dezember 2016 (01.12.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/188637 A1

(51) Internationale Patentklassifikation:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2016/000873

(22) Internationales Anmeldedatum:
25. Mai 2016 (25.05.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2015 006 751.6 26. Mai 2015 (26.05.2015) DE

(71) Anmelder: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder: **HERGET, Werner**; Gänselieselstr. 55, 81739 München (DE). **WERNER, Thomas**; Zennerstr. 14, 81379 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *mit geänderten Ansprüchen gemäss Artikel 19 Absatz 1*

(54) **Title**: METHOD FOR PROVIDING A PERSONAL IDENTIFICATION CODE OF A SECURITY MODULE

(54) **Bezeichnung** : VERFAHREN ZUR BEREITSTELLUNG EINES PERSÖNLICHEN IDENTIFIKATIONSCODES EINES SICHERHEITSMODULS

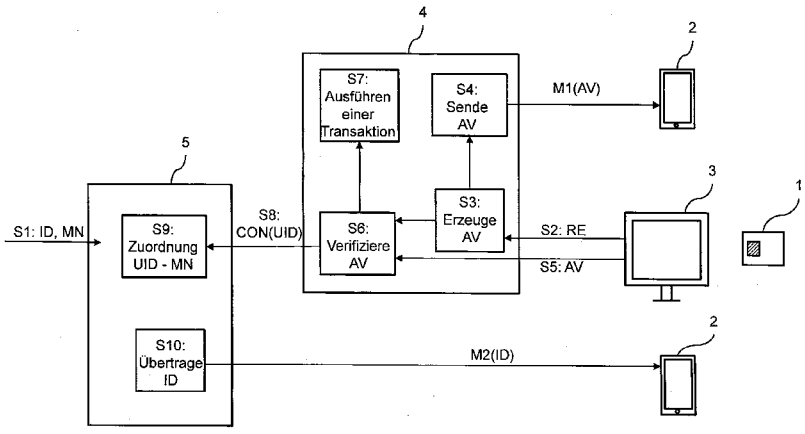

Fig. 1

S9 UID - MN association
S10 Transmit ID
S7 Perform a transaction
S4 Send AV
S6 Check AV
S3 Generate AV

(57) **Abstract**: The invention relates to a method for providing a personal identification code (ID) of a security module (1), wherein the personal identification code (ID) is associated with the security module (1) and there is a server (4) provided which a user of the security module (1) is able to access following an authentication. The method involves, on initiation by a request (RE) from the user on the server (4), an authentication code (AV) being transmitted to a terminal (2) of the user by means of a first message (N1). An authentication code that is input by the user is received on the server (4), and a check is then performed to determine whether the input authentication code matches the authentication code (AV) that has been transmitted to the terminal (2), the personal identification code (ID) being transmitted to the terminal (2) of the user by means of a second message (M2) in the event of a match.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2016/188637 A1

Die Erfindung betrifft ein Verfahren zur Bereitstellung eines persönlichen Identifikationscodes (ID) eines Sicherheitsmoduls (1), wobei der persönliche Identifikationscode (ID) dem Sicherheitsmodul (1) zugewiesen ist und ein Server (4) vorgesehen ist, auf dem ein Benutzer des Sicherheitsmoduls (1) nach einer Authentif ikation zugreifen kann. In dem Verfahren wird, ausgelöst durch eine Anfrage (RE) des Benutzers am Server (4), ein Authentifikationscode (AV) mittels einer ersten Nachricht (M1) an ein Endgerät (2) des Benutzers übermittelt. Ein durch den Benutzer eingegebener Authentifikationscode wird am Server (4) empfangen, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode (AV) übereinstimmt, der an das Endgerät (2) übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode (ID) mittels einer zweiten Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt wird.

Verfahren zur Bereitstellung eines persönlichen Identifikationscodes eines Sicherheitsmoduls

Die Erfindung betrifft ein Verfahren und ein System zur Bereitstellung eines persönlichen Identifikationscodes eines Sicherheitsmoduls.

Sicherheitsmodule, wie z.B. Chipkarten, werden häufig durch persönliche Identifikationscodes bzw. PINs geschützt, die nur dem Inhaber bzw. Benutzer des Sicherheitsmoduls bekannt sind. Dabei sind aus dem Stand der Technik verschiedene Verfahren bekannt, wie der persönliche Identifikationscode dem Benutzer des Sicherheitsmoduls erstmalig bekannt gemacht werden kann. Häufig wird der Identifikationscode dem Benutzer mit einem separaten Brief per Post zugestellt. Dieser separate Versand des Identifikationscodes ist aufwändig und teuer.

Aus der DE 195 07 044 ist das sogenannte "Null-PIN-Verfahren" bekannt, bei dem der Nutzer bei der erstmaligen Inbetriebnahme einer SIM-Karte eine PIN bestehend ausschließlich aus den Ziffernfolge "0000" eingeben muss. Die Eingabe kann bei der erstmaligen Aktivierung der SIM-Karte in einem eigens dafür vorgesehenen Menü erfolgen. Ein solches Menü wird in der DE 198 50 307 beschrieben. Zusätzliche Sicherheit erhält der Nutzer, wenn er die PIN beispielsweise aus den letzten vier Ziffern seiner SIM-Kartennummer oder aus seinem Geburtsdatum ermittelt. Ein derartiges Verfahren wird in der EP 2 053 569 A1 beschrieben.

Nachteil dieser Verfahren ist, dass sowohl die Null-PIN als auch die aus der Kartennummer oder dem Geburtstag gebildete PIN sehr leicht ermittelt werden können und somit eine SIM-Karte, die auf postalischem Wege zugestellt wird und auf böswillige Weise abgefangen wird, sehr leicht missbräuchlich eingesetzt werden kann.

In EP 2 187 363 ist die elektronische Übermittlung einer persönlichen Identifikationsnummer für eine Karte an einen Benutzer der Karte beschrieben. Der Benutzer erhält einen Abfragecode zur Abfrage der persönlichen Identifikationsnummer. Nachdem der Abfragecode durch den Benutzer mittels einer SMS-Nachricht übermittelt wurde, wird die persönliche Identifikationsnummer dem Benutzer wiederum über eine SMS-Nachricht bereitgestellt.

Aufgabe der Erfindung ist es, ein Verfahren und ein System zu schaffen, mit denen auf einfache Weise ein persönlicher Identifikationscode eines Sicherheitsmoduls einem Benutzer bereitgestellt wird.

Diese Aufgabe wird durch den Gegenstand der unabhängigen Ansprüche gelöst. Weiterbildungen der Erfindungen sind in den abhängigen Ansprüchen definiert.

In dem erfindungsgemäßen Verfahren wird ein persönlicher Identifikationscode bereitgestellt, der einem Sicherheitsmodul zugewiesen ist. Dabei wird ein Server verwendet, auf den ein Benutzer (Inhaber) des Sicherheitsmoduls nach einer Authentifikation zugreifen kann. Vorzugsweise erfolgt dieser Zugriff auf den Server über ein Netzwerk, wie das Internet.

Das Sicherheitsmodul ist vorzugsweise ein tragbarer Datenträger. Insbesondere ist der tragbare Datenträger eine Chipkarte, wie z.B. eine Bankkarte bzw. Kreditkarte oder eine SIM/USIM-Karte. Ebenso kann der tragbare Datenträger ein USB-Token oder ein RFID-Transponder sein.

Im Rahmen des Verfahrens wird, ausgelöst durch eine Anfrage des Benutzers am Server, ein Authentifikationscode, der vorzugsweise ein Einmal-Passwort ist, mittels einer ersten Nachricht an ein Endgerät des Benutzers übermittelt.

Ein danach durch den Benutzer eingegebener Authentifikationscode wird am Server empfangen, wobei in einem nächsten Schritt des erfindungsgemäßen Verfahrens verifiziert wird, ob der eingegebene Authentifikationscode mit dem obigen Authentifikationscode übereinstimmt, der an das Endgerät übermittelt wurde. Im Falle einer Übereinstimmung des eingegebenen Authentifikationscodes mit dem übermittelten Authentifikationscode wird schließlich der persönliche Identifikationscode mittels einer zweiten Nachricht an das Endgerät des Benutzers übermittelt. Analog zur ersten Nachricht ist die zweite Nachricht vorzugsweise an eine dem Benutzer zugeordnete Mobilfunknummer adressiert. Insbesondere ist die zweite Nachricht ebenfalls eine SMS-Nachricht. Falls die Authentifikationscodes nicht übereinstimmen, wird das Aussenden der zweiten Nachricht unterbunden.

Mit dem erfindungsgemäßen Verfahren wird auf einfache Weise mittels eines Servers eine elektronische Übermittlung des persönlichen Identifikationscodes an ein Endgerät des Benutzers erreicht. Das Verfahren ist dabei besonders sicher, da die Übertragung des persönlichen Identifikationscodes an einen Authentifikationscode gekoppelt ist, der vom Server empfangen wird und zuvor an das Endgerät des Benutzers übertragen wurde. Das Verfahren zur Übermittlung des persönlichen Identifikationscodes wird durch die Anfrage des Benutzers am Server angestoßen/initiiert.

Das Endgerät ist vorzugsweise ein mobiles Endgerät, insbesondere ein Mobilfunkgerät. Das Endgerät weist vorzugsweise zumindest eine Netzwerk-

schnittstelle (Mobilfunk-, WLAN-, Internet-Schnittstelle) auf. Die erste Nachricht ist in einer bevorzugten Variante an eine dem Endgerät (oder dem Benutzer) zugeordnete Kommunikationsnummer, wie Mobilfunknummer oder IP-Adresse, adressiert. Insbesondere kann die erste Nachricht eine an sich bekannte SMS-Nachricht bzw. Kurznachricht (SMS = Short Message Service) sein. Alternativ kann die erste Nachricht beispielsweise eine Internetnachricht sein, die an eine Applikation (App, beispielsweise eine Messenger-App) des Endgerätes übertragen wird.

Die Authentifizierung (bzw. Anmeldung) des Benutzers beim Server kann auf beliebigem Weg erfolgen, z.b. durch Benutzername und Passwort, durch biometrische Merkmale oder mittels einer Authentisierungsanwendung auf einem anderen (oder demselben) Sicherheitsmodul.

Der Benutzer ist in einer bevorzugten Ausgestaltung für die Authentisierung (Anmeldung) des Benutzers am Server bereits vorab registriert. Besonders bevorzugt ist das Endgerät des Benutzers beim Server bereits vorab mit seiner Kommunikationsnummer registriert. In einer besonders bevorzugten Ausführungsform ist der im erfindungsgemäßen Verfahren verwendete Server ein Online-Transaktions-Server, z.B. ein Online-Banking-System eines Kreditinstituts bzw. einer Bank. Mittels eines solchen Servers können elektronisch Transaktionen (wie z.B. monetäre Transaktionen) durchgeführt werden. Ein solcher Server enthält schon entsprechende Komponenten, welche das Übermitteln eines Authentifikationscodes sowie die Verifikation eines Authentifikationscodes im Rahmen einer Online-Transaktion ermöglichen. Der Online-Transaktions-Server enthält die vorab registrierten Authentisierungsdaten des Benutzers. Diese Komponenten und/oder Authentisierungsdaten können nunmehr im erfindungsgemäßen Verfahren zur Bereit-

stellung eines persönlichen Identifikationscodes für ein Sicherheitsmodul genutzt werden.

In einer besonders bevorzugten Ausführungsform verwendet der soeben beschriebene Online-Transaktions-Server Transaktionscodes, beispielsweise als TAN oder OTP, zur Verifikation von durch den Benutzer veranlassten Transaktionen, wobei in Antwort auf die Anfrage des Benutzers als Authentifikationscode ein Transaktionscode mittels der ersten Nachricht an das Endgerät des Benutzers übermittelt wird. Es wird somit ein an sich bekanntes TAN-Verfahren bzw. smsTAN-Verfahren eines Online-Transaktions-Servers zur Bereitstellung des persönlichen Identifikationscodes genutzt.

In einer weiteren bevorzugten Ausführungsform wird die erste und/oder zweite Nachricht von einer Bereitstellungsinstanz (d.h. einem separaten Server), die mit dem obigen Server kommuniziert, an das Endgerät des Benutzers übermittelt.

Der Herausgeber des Sicherheitsmoduls, für welches das erfindungsgemäße Verfahren den persönlichen Identifikationscode bereitstellt, kann ggf. auch der Betreiber des Servers sein. Nichtsdestotrotz können der Herausgeber des Sicherheitsmoduls und der Betreiber des Servers auch zwei unterschiedliche Instanzen sein, wie z.B. zwei unterschiedliche Banken. Ebenso kann die Bereitstellungsinstanz eine von dem Herausgeber des Sicherheitsmoduls bzw. dem Betreiber des Servers unabhängige Instanz sein. Es kann sich hierbei z.B. um den Hersteller des Sicherheitsmoduls handeln.

In einer besonders bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird der Authentifikationscode in dem Server generiert. Vorzugsweise wird der im Server generierte Authentifikationscode auch durch

den Server mittels der ersten Nachricht an das Endgerät des Benutzers übermitteln.

In einer weiteren Variante des erfindungsgemäßen Verfahrens, welche die oben beschriebene Bereitstellungsinstanz verwendet, wird der im Server generierte Authentifikationscode durch den Server an die Bereitstellungsinstanz übermittelt, welche den übermittelten Authentifikationscode mittels der ersten Nachricht an das Endgerät des Benutzers übermittelt.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens weist der Server die Bereitstellungsinstanz an, den Authentifikationscode zu generieren, woraufhin die Bereitstellungsinstanz den Authentifikationscode erzeugt und an das Endgerät des Benutzers mittels der ersten Nachricht übermittelt.

In einer besonders bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät übermittelten Authentifikationscode durch den Server selbst. Bei Verwendung der Bereitstellungsinstanz übernimmt diese Instanz in einer bevorzugten Variante der soeben beschriebenen Ausführungsform das Übermitteln der zweiten Nachricht. Mit anderen Worten wird im Falle einer Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät übermittelten Authentifikationscode der Bereitstellungsinstanz eine Bestätigung durch den Server bereitgestellt, wobei die Bereitstellungsinstanz in Antwort auf die Bereitstellung der Bestätigung die zweite Nachricht an das Endgerät des Benutzers übermittelt. Die Bereitstellung der Bestätigung kann durch eine Übermittlung der Bestätigung von dem Server an die Bereitstellungsinstanz erfolgen. Ebenso kann die Bereitstellung der Bestätigung in der Form einer durch den

Server durchgeführten Transaktion erfolgen. Die Bestätigung kann ggf. eine Benutzerkennung bzw. Benutzeridentifikation des Benutzers umfassen. Ferner kann die Bestätigung ggf. den Authentifikationscode umfassen.

In einer weiteren bevorzugten Variante des erfindungsgemäßen Verfahrens stellt der Server dem Benutzer eine Eingabemaske für den Authentifikationscode bereit.

Wird im erfindungsgemäßen Verfahren die obige Bereitstellungsinstanz verwendet, kann in einer weiteren Ausgestaltung die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät übermittelten Authentifikationscode auch durch die Bereitstellungsinstanz erfolgen, wobei die Bereitstellungsinstanz im Falle einer Übereinstimmung die zweite Nachricht an das Endgerät des Benutzers übermittelt.

In einer weiteren bevorzugten Variante der Erfindung, bei der die erste und zweite Nachricht an eine dem Benutzer zugeordnete Kommunikationsnummer adressiert sind, ist diese Kommunikationsnummer vorab, d.h. vor Durchführung des erfindungsgemäßen Verfahrens, in einem Speicher hinterlegt. Aus diesem Speicher wird die Kommunikationsnummer zur Übermittlung der ersten und zweiten Nachricht ausgelesen. Nichtsdestotrotz besteht auch die Möglichkeit, dass die dem Benutzer zugeordnete Kommunikationsnummer während der Durchführung des erfindungsgemäßen Verfahrens von dem Benutzer an den Server übermittelt wird. Mit anderen Worten wird im Rahmen der Durchführung des Verfahrens die Kommunikationsnummer über den Server beim Benutzer abgefragt und durch diesen am Server eingegeben. Die Übermittlung der Kommunikationsnummer kann z.B. zusammen mit der obigen Anfrage des Benutzers am Server erfolgen.

In einer weiteren Ausführungsform wird das erfindungsgemäße Verfahren in Kombination mit einem Sicherheitsmodul verwendet, dem ein oder mehrere initiale Identifikationscodes zugewiesen sind, die häufig auch als Transport-PINs bezeichnet werden. Dabei ist bei Auslieferung des Sicherheitsmoduls der initiale Identifikationscode oder ein einzelner der initialen Identifikationscodes aktiviert und dieser aktivierte initiale Identifikationscode wird als persönlicher Identifikationscode durch das erfindungsgemäße Verfahren bereitgestellt. Der Benutzer kann mit dem an sein Endgerät übermittelten aktivierten initialen Identifikationscode einen neuen persönlichen Identifikationscode für das Sicherheitsmodul einrichten. Im Falle, dass dem Sicherheitsmodul mehrere Identifikationscodes zugewiesen sind, wird in einer bevorzugten Variante ein anderer initialer Identifikationscode aktiviert, sofern ein initialer, zuvor aktivierter Identifikationscode oder ein durch den Benutzer neu eingerichteter persönlicher Identifikationscode blockiert wird.

Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein System zur Bereitstellung eines persönlichen Identifikationscodes eines Sicherheitsmoduls, wobei der persönliche Identifikationscode dem Sicherheitsmodul zugewiesen ist. Das System umfasst einen Server, auf den der Benutzer des Sicherheitsmoduls nach einer Authentifikation zugreifen kann. Das System ist dabei zur Durchführung eines Verfahrens eingerichtet, bei dem:

- ausgelöst durch eine Anfrage des Benutzers am Online-Portal ein Authentifikationscode mittels einer ersten Nachricht an ein Endgerät des Benutzers übermittelt wird;
- ein durch den Benutzer eingegebener Authentifikationscode am Server empfangen wird, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode übereinstimmt,

der an das Endgerät übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode mittels einer zweiten Nachricht an das Endgerät des Benutzers übermittelt wird.

In einer bevorzugten Ausführungsform ist das erfindungsgemäße System zur Durchführung einer oder mehrerer bevorzugter Varianten des erfindungsgemäßen Verfahrens eingerichtet.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der beigefügten Figuren detailliert beschrieben.

Es zeigen:

Fig.1 eine schematische Darstellung einer ersten Variante des erfindungsgemäßen Verfahrens; und

Fig. 2 eine schematische Darstellung einer zweiten Variante des erfindungsgemäßen Verfahrens.

Im Folgenden werden Ausführungsformen der Erfindung anhand eines persönlichen Identifikationscodes in der Form einer PIN einer Chipkarte 1 beschrieben. Die PIN ist in Fig. 1 mit dem Bezugszeichen ID bezeichnet. Die Chipkarte 1 stellt dabei eine Bankkarte bzw. Kreditkarte einer Bank dar. Die Karte muss nicht notwendigerweise einen Chip enthalten. Mittels der PIN kann der Benutzer der Chipkarte 1 (d.h. der Karteninhaber) monetäre Transaktionen authentifizieren. Zum Beispiel kann er durch Eingabe der PIN an einem Bank-Terminal, in dem die Chipkarte 1 eingeschoben ist, Geld abheben.

Herkömmlicherweise wird dem Benutzer der Chipkarte 1 die zu der Karte gehörige PIN auf postalischem Weg mitgeteilt. In den hier beschriebenen Ausführungsformen erfolgt die Übermittlung der PIN in elektronischer Form unter Einbeziehung eines Servers in der Form eines Online-Banking-Systems 4. Das Online-Banking-System gehört in der hier beschriebenen Ausführungsform zu der Bank, welche die Karte 1 herausgegeben hat. Nichtsdestotrotz kann das Online-Banking-System auch zu einer anderen Bank gehören, welche nicht der Bank des Herausgebers der Chipkarte 1 entspricht. Ferner ist es auch möglich, dass der Herausgeber der Chipkarte 1 die weiter unten beschriebene Bereitstellungsinstanz 5 ist. Gegebenenfalls können der Herausgeber der Karte 1, das Online-Banking-System 4 und die Bereitstellungsinstanz 5 drei unabhängige Instanzen sein.

Das Online-Banking-System 4 basiert auf einem herkömmlichen Online-Transaktions-Server, mit dem monetäre Transaktionen (Überweisungen, Buchungen, Gutschriften) durchgeführt werden, die von einem Benutzer über ein Endgerät 3 am Online-Banking-System 4 spezifiziert wurden. Dabei wird das an sich bekannte smsTAN-Verfahren genutzt, bei dem vor der Durchführung einer Transaktion ein Authentifikationscode in dem Online-Banking-System 4 erzeugt wird und mittels einer SMS-Nachricht an ein Mobilfunkgerät 2 des Benutzers übermittelt wird. Dieser gibt den Authentifikationscode dann über das Endgerät 3 an dem Online-Banking-System 4 ein, welches die Transaktion nur bei Übereinstimmung des eingegebenen Authentifikationscodes mit dem zuvor an das Mobilfunkgerätgerät 2 übermittelten Authentifikationscode durchführt. Gemäß der Ausführungsform der Fig. 1 wird die Funktionalität des smsTAN-Verfahrens nunmehr für den neuen Zweck der elektronischen Übermittlung der PIN ID an den Benutzer genutzt.

Im Rahmen der Durchführung des Verfahrens der Fig. 1 wird neben der PIN ID eine Mobilfunknummer MN in der Form einer MSISDN benötigt, die dem Mobilfunkgerät 2 des Benutzers der Chipkarte 1 zugeordnet ist. Gemäß Fig. 1 sind sowohl die PIN ID als auch die Mobilfunknummer MN vorab in einer Bereitstellungsinstanz 5 in der Form eines weiteren Servers gespeichert, wie durch den entsprechenden Schritt S1 angedeutet ist. Die PIN bzw. die Mobilfunknummer werden über einen sicheren Kanal an die Bereitstellungsinstanz 5 übermittelt. Die PIN und die Mobilfunknummer stammen im hier beschriebenen Ausführungsbeispiel von der Bank, welche die Chipkarte 1 herausgegeben hat und welche auch das Online-Banking-System 4 betreibt. Die Mobilfunknummer MN wurde dabei vorab bei der Bank registriert und ist auch im Online-Banking-System 4 hinterlegt. Die in der Bereitstellungsinstanz 5 gespeicherte Mobilfunknummer kann nach Durchführung des Verfahrens ggf. wieder gelöscht werden bzw. bei einer Veränderung aktualisiert werden.

In einer alternativen Variante braucht die Mobilfunknummer MN auch nicht vorab in dem Online-Banking-System 4 bzw. der Bereitstellungsinstanz 5 hinterlegt sein, sondern sie kann während der Durchführung des Verfahrens dem Online-Banking-System 4 bzw. der Bereitstellungsinstanz 5 bereitgestellt werden. Vorzugsweise wird die Mobilfunknummer dabei durch den Karteninhaber am Online-Banking-System 4 eingegeben. Die Mobilfunknummer steht somit dem Online-Banking-System 4 zur Verfügung, welches die Nummer auch an die Bereitstellungsinstanz 5 übermittelt. In diesem Fall muss nicht mehr zwischen vorab registrierten Mobilfunknummern und neu eingegebenen Mobilfunknummern unterschieden werden, denn die Mobilfunknummer wird immer durch den Benutzer spezifiziert. Darüber hinaus müssen keine Funktionalitäten zum Löschen bzw. zur Aktualisierung der Mobilfunknummer vorgesehen werden.

Gemäß der Ausführungsform der Fig. 1 ist der Benutzer der Chipkarte 1 mittels einer entsprechenden Authentifizierung an dem Online-Banking-System 4 über das Internet eingeloggt. Dabei verwendet der Benutzer das internetfähige Endgerät 3 (z.B. einen Computer), über das er mittels eines Browsers auf das Online-Banking-System 4 zugreift. Zunächst gibt der Benutzer in Schritt S2 am Online-Banking-System 4 eine Anfrage RE zur elektronischen Bereitstellung der zur Karte 1 gehörigen PIN ID ein. Das Online-Banking-System 4 erzeugt daraufhin in Schritt S3 einen Authentifikationscode AV (AV = Authentication Value). Dieser Authentifikationscode ist eine an sich bekannter Transaktionscode in der Form einer TAN (oder eines Einmalpasswortes), die herkömmlicherweise zur Authentifizierung von monetären Transaktionen am Online-Banking-System genutzt wird. Der Transaktionscode kann auch als Transaktionsfreigabecode bezeichnet werden.

Der Authentifikationscode AV wird anschließend in einem Schritt S4 durch den Server 4 an das Mobilfunkgerät 2 des Benutzers gesendet. Dies erfolgt mittels der Übertragung einer SMS-Nachricht M1, welche unter Verwendung der bekannten Mobilfunknummer MN an das Mobilfunkgerät 2 des Benutzers gesendet wird. Anstelle einer SMS kann hier und auch im Folgenden eine Internetnachricht z.b. an eine (Messenger-)App auf dem Mobilfunkgerät übertragen werden. Der Authentifikationscode AV ist nur zur einmaligen Verwendung (d.h. als Einmal-Passwort) vorgesehen. Somit müssen keine erhöhten Sicherheitsanforderungen im Rahmen der Übermittlung der SMS-Nachricht M1 in Schritt S4 vorgesehen werden, denn der Lebenszyklus des Authentifikationscodes AV ist sehr kurz. Im Besonderen muss nicht überprüft werden, ob die SMS auch zugestellt wurde, denn dieser Prozess kann jederzeit wieder gestartet werden. Es kann somit ein herkömmlicher SMS-

Aggregator zum Aussenden des Authentifikationscodes AV eingesetzt werden.

Nach Zustellung der Nachricht M1 liest der Benutzer den Authentifikationscode AV von dem Display des Mobilfunkgeräts 2 ab und gibt ihn in Schritt S5 mittels des Endgeräts 3 an dem Online-Banking-System 4 ein, und zwar wie dies üblicherweise im Rahmen der Eingabe einer smsTAN erfolgt. Der Authentifikationscode AV wird dann in Schritt S6 im Server 4 verifiziert. Das heißt, der Server 4 überprüft, ob der zuvor in Schritt S3 erzeugte Authentifikationscode mit dem in Schritt S5 erhaltenen Authentifikationscode übereinstimmt. Ist dies der Fall, war die Verifikation des Authentifikationscodes AV erfolgreich. Falls der Authentifikationscode im Rahmen einer herkömmlichen monetären Transaktion verwendet worden wäre, würde diese Transaktion in Schritt S7 ausgeführt werden, falls die Verifikation in Schritt S6 erfolgreich war. In dem Ausführungsbeispiel der Fig. 1 ist an die erfolgreiche Verifikation des Authentifikationscodes in Schritt S6 nunmehr der Schritt S8 gekoppelt, in dem eine Bestätigung CON, welche eine Benutzeridentifikation UID des Benutzers umfasst, von dem Server 4 an die Bereitstellungsinstanz 5 über eine gesicherte Schnittstelle übermittelt wird.

In der Bereitstellungsinstanz 5 sind Verknüpfungen zwischen Benutzeridentifikationen und Mobilfunknummern hinterlegt. Basierend auf diesen Verknüpfungen ordnet die Bereitstellungsinstanz 5 in Schritt S9 die Benutzeridentifikation UID, die zuvor in Schritt S8 übertragen wurde, der Mobilfunknummer MN zu. Anschließend sendet die Bereitstellungsinstanz 5 in Schritt S10 die PIN ID, welche ihr in Schritt S1 bereitgestellt wurde, an das Mobilfunkgerät 2 des Benutzers. Dies erfolgt wiederum über das Aussenden einer SMS-Nachricht M2, welche die PIN ID enthält. Zwecks übersichtlicher Darstellung ist in Fig. 1 und auch in der weiter unten beschriebenen Fig. 2 das

Mobilfunkgerät 2 des Benutzers im Zusammenhang mit der Übermittlung der Nachricht M2 nochmals dargestellt.

Der Benutzer erhält somit auf elektronischem Weg die PIN für seine Karte 1 und kann dann anschließend entsprechende Transaktionen mittels der Karte und der übermittelten PIN durchführen. Da entsprechende Authentifizierungen und Verifikationen bereits vorab durchgeführt wurden, müssen auch keine speziellen Sicherheitsanforderungen für die Übermittlung der SMS in Schritt S10 implementiert werden. Vielmehr kann ein herkömmlicher SMS-Aggregator zur Übertragung der SMS eingesetzt werden.

In einer sicheren Ausgestaltung wird der Authentifikationscodes AV in Schritt S4 nur ein einziges Mal gesendet. Ebenso bzw. zusätzlich kann es vorgesehen sein, für die in Schritt S1 übermittelte PIN nur einmal eine Anforderung S2 und/oder nur einmal eine Übertragung S10 zuzulassen. Eine zweite Anforderung S2, Sendung S4 und/oder Übertragung S10 würde dann ein erneutes Übermitteln S1 der PIN oder eine nicht dargestellte Freigabe für einen erneuten Ablauf des Verfahrens (mit den Schritten S2 bis S10) erfordern.

In einer abgewandelten Variante des Verfahrens der Fig. 1 wird der Bereitstellungsinstanz 5 die Betätigung über eine erfolgreiche Verifikation des Authentifikationscodes nicht unmittelbar mittels der Übertragung einer Benutzeridentifikation (Schritt S8) mitgeteilt. Vielmehr ist die erfolgreiche Verifikation des Authentifikationscodes an die Durchführung einer speziellen Transaktion (z.B. die Überweisung von einem Cent) an eine spezielle Nummer eines Kontos gekoppelt, auf welches die Bereitstellungsinstanz 5 Zugriff hat. Diese spezielle Transaktion wird im entsprechenden Schritt S7 durchgeführt. Sobald die Bereitstellungsinstanz 5 die Durchführung dieser speziellen

Transaktion feststellt, überträgt sie die PIN ID an die Mobilfunknummer MN des Mobilfunkgeräts 2 mittels der entsprechenden SMS-Nachricht M2.

Fig. 2 zeigt eine zweite Variante des erfindungsgemäßen Verfahrens. In dieser Variante übernimmt die Bereitstellungsinstanz 5 Funktionen, die in der Ausführungsform der Fig. 1 von dem Server 4 durchgeführt werden. Analog zu Schritt S1 der Fig. 1 werden in Schritt S101 sowohl die PIN ID als auch die Mobilfunknummer MN vorab in der Bereitstellungsinstanz 5 bereitgestellt. In Schritt S102 gibt der Benutzer - analog zu Schritt S2 der Fig. 1 - am Online-Banking-System 4 eine Anfrage RE zur elektronischen Bereitstellung der zur Karte 1 gehörigen PIN ID ein. Das Online-Banking-System 4 erzeugt daraufhin den entsprechenden Authentifikationscode AV, der in Schritt S103 von dem Online-Banking-System 4 an die Bereitstellungsinstanz 5 über eine gesicherte Schnittstelle übermittelt wird. Durch die Übermittlung des Authentifikationscodes AV in Schritt S103 wird in der Bereitstellungsinstanz 5 das Aussenden dieses Codes mittels der SMS-Nachricht M1 an das Mobilfunkgerät 2 des Benutzers ausgelöst (Schritt S104).

In Analogie zu dem Verfahren der Fig. 1 liest der Benutzer den mit der Nachricht M1 übermittelten Authentifikationscode AV von dem Display des Mobilfunkgeräts 2 ab und gibt ihn in Schritt S105 mittels des Endgeräts 3 an dem Online-Banking-System 4 ein. Der Authentifikationscode AV wird dann in Schritt S106 über die gesicherte Schnittstelle an die Bereitstellungsinstanz 5 übermittelt, die den Authentifikationscode in Schritt S107 verifiziert, d.h. sie überprüft, ob der zuvor in Schritt S103 übermittelte Authentifikationscode mit dem in Schritt S106 erhaltenen Authentifikationscode übereinstimmt. Ist dies der Fall, überträgt die Bereitstellungsinstanz 5 in Schritt S108 die PIN ID mittels der SMS-Nachricht M2 an die Mobilfunknummer des Mobilfunkgeräts 2.

In einer abgewandelten Variante des Verfahrens der Fig. 2 kann in Schritt S103 auch lediglich ein Sendebefehl ohne Authentifikationscode an die Bereitstellungsinstanz 5 übermittelt werden. In Reaktion auf den Sendebefehl wird dann der Authentifikationscode durch die Bereitstellungsinstanz 5 selbst erzeugt, welche diesen Code dann wiederum in Schritt S104 mittels einer Kurznachricht an das Endgerät 2 sendet.

Das erfindungsgemäße Verfahren kann z.B. in Kombination mit sog. Transport-PINs eingesetzt werden, die vor dem Versand der Chipkarte an den Benutzer darauf hinterlegt werden. Dabei ist nur eine der Transport-PINs aktiv. Mittels des soeben beschriebenen Verfahrens wird dem Benutzer bzw. Karteninhaber diese aktive Transport-PIN elektronisch übermittelt. Die übermittelte Transport-PIN wird dann von dem Karteninhaber bei der erstmaligen Verwendung der Karte, z.B. an einem Bank-Terminal, genutzt. Der Karteninhaber kann dann im Rahmen dieser erstmaligen Verwendung die aktuelle Transport-PIN inaktiv schalten bzw. löschen, indem er eine neue PIN spezifiziert. Wird diese PIN zu einem späteren Zeitpunkt geblockt, kann das oben beschriebene Verfahren für eine andere Transport-PIN auf der Karte wiederholt werden. In der Karte ist dabei eine Reihenfolge hinterlegt, in der die Transport-PINs aktiv geschaltet werden. Das heißt, es ist hinterlegt, welche Transport-PIN als nächstes aktiviert wird, falls eine vorhergehende Transport-PIN inaktiv wird.

Die im Vorangegangenen beschriebenen Ausführungsformen der Erfindung weist eine Reihe von Vorteilen auf. Insbesondere wird auf einfache Weise unter Verwendung eines Online-Portals bzw. eines Online-Banking-Systems die elektronische Übermittlung einer Chipkarten-PIN erreicht. Dabei macht man sich insbesondere das an sich bekannte smsTAN-Verfahren zunutze, bei

dem die elektronische Übermittlung der PIN erst dann veranlasst wird, wenn eine zuvor mittels einer SMS übermittelte TAN durch einen Benutzer an dem Online-Banking-System eingegeben wurde.

Patentansprüche

1. Verfahren zur Bereitstellung eines persönlichen Identifikationscodes (ID) eines Sicherheitsmoduls (1), wobei der persönliche Identifikationscode (ID) dem Sicherheitsmodul (1) zugewiesen ist und ein Server (4) vorgesehen ist, auf den ein Benutzer des Sicherheitsmoduls (1) nach einer Authentifikation zugreifen kann, bei dem:
   - ausgelöst durch eine Anfrage (RE) des Benutzers am Server (4) ein Authentifikationscode (AV) mittels einer ersten Nachricht (M1) an ein Endgerät (2) des Benutzers übermittelt wird;
   - ein durch den Benutzer eingegebener Authentifikationscode (AV) am Server (4) empfangen wird, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode übereinstimmt, der an das Endgerät (2) übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode (ID) mittels einer zweiten Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Server (4) ein Online-Transaktions-Server ist.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass der Online-Transaktions-Server Transaktionscodes zur Verifikation von durch den Benutzer veranlassten Transaktionen verwendet, wobei in Antwort auf die Anfrage (RE) des Benutzers als Authentifikationscode (AV) ein Transaktionscode mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste und/oder zweite Nachricht (M1, M2) von einer Bereitstellungsinstanz (5), die mit dem Server (4) kommuniziert, an das Endgerät (2) des Benutzers übermittelt werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Authentifikationscode (AV) in dem Server (4) generiert wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass der im Server (4) generierte Authentifikationscode (AV) durch den Server (4) mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4 und 5, dadurch gekennzeichnet, dass der im Server (4) generierte Authentifikationscode (AV) durch den Server (4) an die Bereitstellungsinstanz (5) übermittelt wird, welche den übermittelten Authentifikationscode (AV) mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt.

8. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass der Server (4) die Bereitstellungsinstanz (5) anweist, den Authentifikationscode (AV) zu generieren, woraufhin die Bereitstellungsinstanz (5) den Authentifikationscode (AV) erzeugt und an das Endgerät (2) des Benutzers mittels der ersten Nachricht (M1) übermittelt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) durch den Server (4) erfolgt.

10. Verfahren nach Anspruch 9 in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass im Falle einer Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) der Bereitstellungsinstanz (5) eine Bestätigung (CON) durch den Server (4) bereitgestellt wird, wobei die Bereitstellungsinstanz (5) in Antwort auf die Bereitstellung der Betätigung (CON) die zweite Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Bestätigung (CON) von dem Server (4) an die Bereitstellungsinstanz (5) übermittelt wird oder in der Form einer durch den Server (4) durchgeführten Transaktion bereitgestellt wird.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Server (4) dem Benutzer eine Eingabemaske für den Authentifikationscode (AV) bereitstellt.

13. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) durch die Bereitstellungsinstanz (5) erfolgt, wobei die Bereitstellungs-

instanz (5) im Falle einer Übereinstimmung die zweite Nachricht M2) an das Endgerät (2) des Benutzers übermittelt.

14. System zur Bereitstellung eines persönlichen Identifikationscodes (ID) eines Sicherheitsmoduls (1), wobei der persönliche Identifikationscode (ID) dem Sicherheitsmodul (1) zugewiesen ist, wobei das System einen Server (4) umfasst, auf den der Benutzer des Sicherheitsmoduls (1) nach einer Authentifikation zugreifen kann, wobei das System zur Durchführung eines Verfahrens eingerichtet ist, bei dem:

- ausgelöst durch eine Anfrage (RE) des Benutzers am Server (4) ein Authentifikationscode (AV) mittels einer ersten Nachricht (M1) an ein Endgerät (2) des Benutzers übermittelt wird;
- ein durch den Benutzer eingegebener Authentifikationscode am Server (4) empfangen wird, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode (AV) übereinstimmt, der an das Endgerät (2) übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode (ID) mittels einer zweiten Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt wird.

15. System nach Anspruch 14, dadurch gekennzeichnet, dass das System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 13 eingerichtet ist.

GEÄNDERTE ANSPRÜCHE
beim Internationalen Büro eingegangen am 01. September 2016

Patentansprüche

1. Verfahren zur Bereitstellung eines persönlichen Identifikationscodes (ID) eines Sicherheitsmoduls (1), wobei der persönliche Identifikationscode (ID) dem Sicherheitsmodul (1) zugewiesen ist und ein Server (4) vorgesehen ist, auf den ein Benutzer des Sicherheitsmoduls (1) nach einer Authentifikation zugreifen kann, bei dem:
   - ausgelöst durch eine Anfrage (RE) des Benutzers am Server (4) ein Authentifikationscode (AV), der ein Einmal-Passwort ist, mittels einer ersten Nachricht (M1) an ein Endgerät (2) des Benutzers übermittelt wird;
   - ein durch den Benutzer eingegebener Authentifikationscode (AV) am Server (4) empfangen wird, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode übereinstimmt, der an das Endgerät (2) übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode (ID) mittels einer zweiten Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Server (4) ein Online-Transaktions-Server ist.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass der Online-Transaktions-Server Transaktionscodes zur Verifikation von durch den Benutzer veranlassten Transaktionen verwendet, wobei in Antwort auf die Anfrage (RE) des Benutzers als Authentifikationscode (AV) ein Transaktionscode mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste und/oder zweite Nachricht (M1, M2) von einer Bereitstellungsinstanz (5), die mit dem Server (4) kommuniziert, an das Endgerät (2) des Benutzers übermittelt werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Authentifikationscode (AV) in dem Server (4) generiert wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass der im Server (4) generierte Authentifikationscode (AV) durch den Server (4) mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4 und 5, dadurch gekennzeichnet, dass der im Server (4) generierte Authentifikationscode (AV) durch den Server (4) an die Bereitstellungsinstanz (5) übermittelt wird, welche den übermittelten Authentifikationscode (AV) mittels der ersten Nachricht (M1) an das Endgerät (2) des Benutzers übermittelt.

8. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass der Server (4) die Bereitstellungsinstanz (5) anweist, den Authentifikationscode (AV) zu generieren, woraufhin die Bereitstellungsinstanz (5) den Authentifikationscode (AV) erzeugt und an das Endgerät (2) des Benutzers mittels der ersten Nachricht (M1) übermittelt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) durch den Server (4) erfolgt.

10. Verfahren nach Anspruch 9 in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass im Falle einer Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) der Bereitstellungsinstanz (5) eine Bestätigung (CON) durch den Server (4) bereitgestellt wird, wobei die Bereitstellungsinstanz (5) in Antwort auf die Bereitstellung der Betätigung (CON) die zweite Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Bestätigung (CON) von dem Server (4) an die Bereitstellungsinstanz (5) übermittelt wird oder in der Form einer durch den Server (4) durchgeführten Transaktion bereitgestellt wird.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Server (4) dem Benutzer eine Eingabemaske für den Authentifikationscode (AV) bereitstellt.

13. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4, dadurch gekennzeichnet, dass die Überprüfung der Übereinstimmung des eingegebenen Authentifikationscodes mit dem an das Endgerät (2) übermittelten Authentifikationscode (AV) durch die Bereitstellungsinstanz (5) erfolgt, wobei die Bereitstellungs-

instanz (5) im Falle einer Übereinstimmung die zweite Nachricht M2) an das Endgerät (2) des Benutzers übermittelt.

14. System zur Bereitstellung eines persönlichen Identifikationscodes (ID) eines Sicherheitsmoduls (1), wobei der persönliche Identifikationscode (ID) dem Sicherheitsmodul (1) zugewiesen ist, wobei das System einen Server (4) umfasst, auf den der Benutzer des Sicherheitsmoduls (1) nach einer Authentifikation zugreifen kann, wobei das System zur Durchführung eines Verfahrens eingerichtet ist, bei dem:

- ausgelöst durch eine Anfrage (RE) des Benutzers am Server (4) ein Authentifikationscode (AV), der ein Einmal-Passwort ist, mittels einer ersten Nachricht (M1) an ein Endgerät (2) des Benutzers übermittelt wird;
- ein durch den Benutzer eingegebener Authentifikationscode am Server (4) empfangen wird, woraufhin verifiziert wird, ob der eingegebene Authentifikationscode mit dem Authentifikationscode (AV) übereinstimmt, der an das Endgerät (2) übermittelt wurde, wobei im Falle einer Übereinstimmung der persönliche Identifikationscode (ID) mittels einer zweiten Nachricht (M2) an das Endgerät (2) des Benutzers übermittelt wird.

15. System nach Anspruch 14, dadurch gekennzeichnet, dass das System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 13 eingerichtet ist.

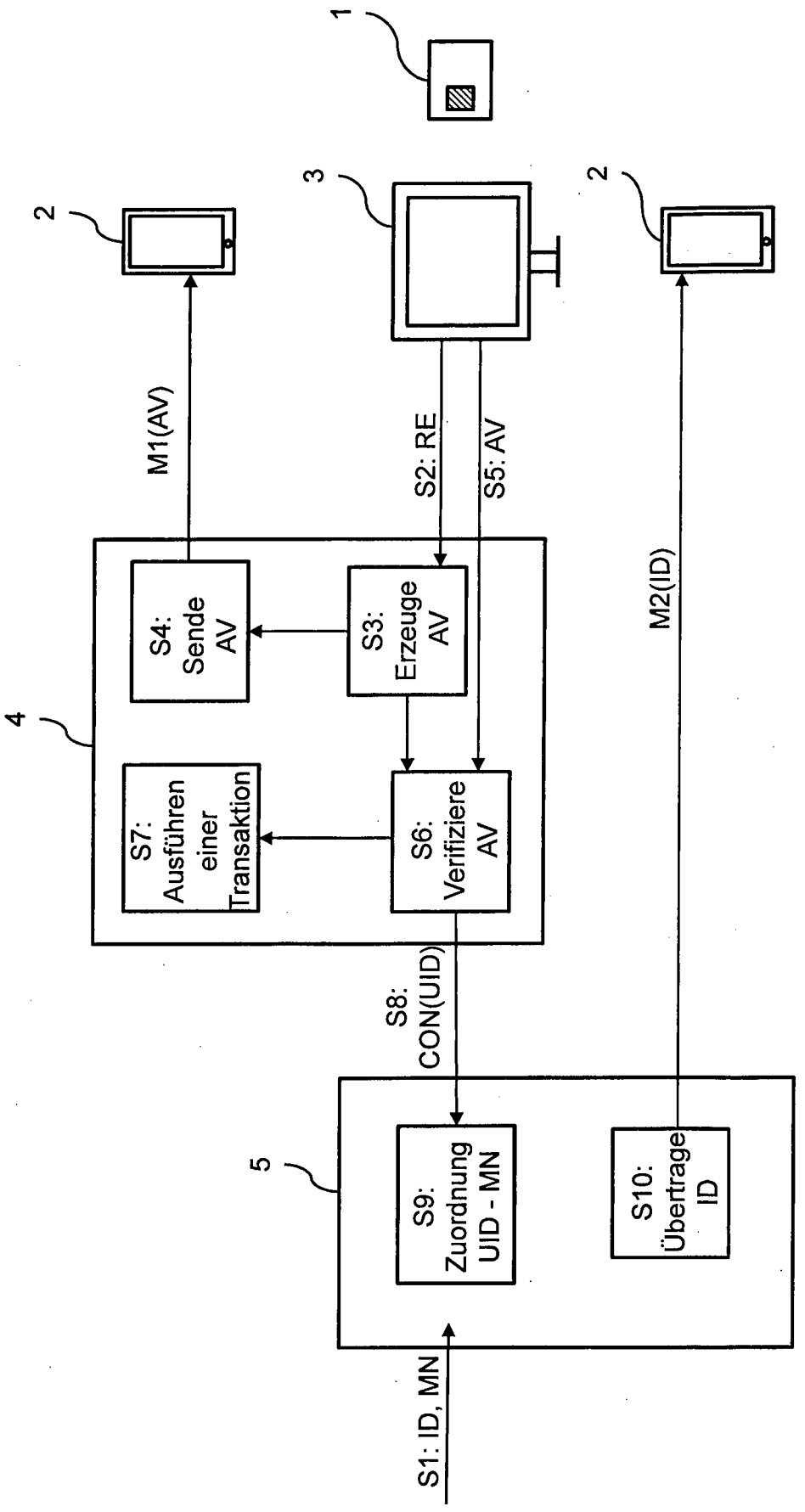
1
2
3
2
M1(AV)
S2: RE
S5: AV
M2(ID)
4
S4: Sende AV
S3: Erzeuge AV
S7: Ausführen einer Transaktion
S6: Verifiziere AV
S8: CON(UID)
5
S9: Zuordnung UID - MN
S10: Übertrage ID
S1: ID, MN

Fig. 1

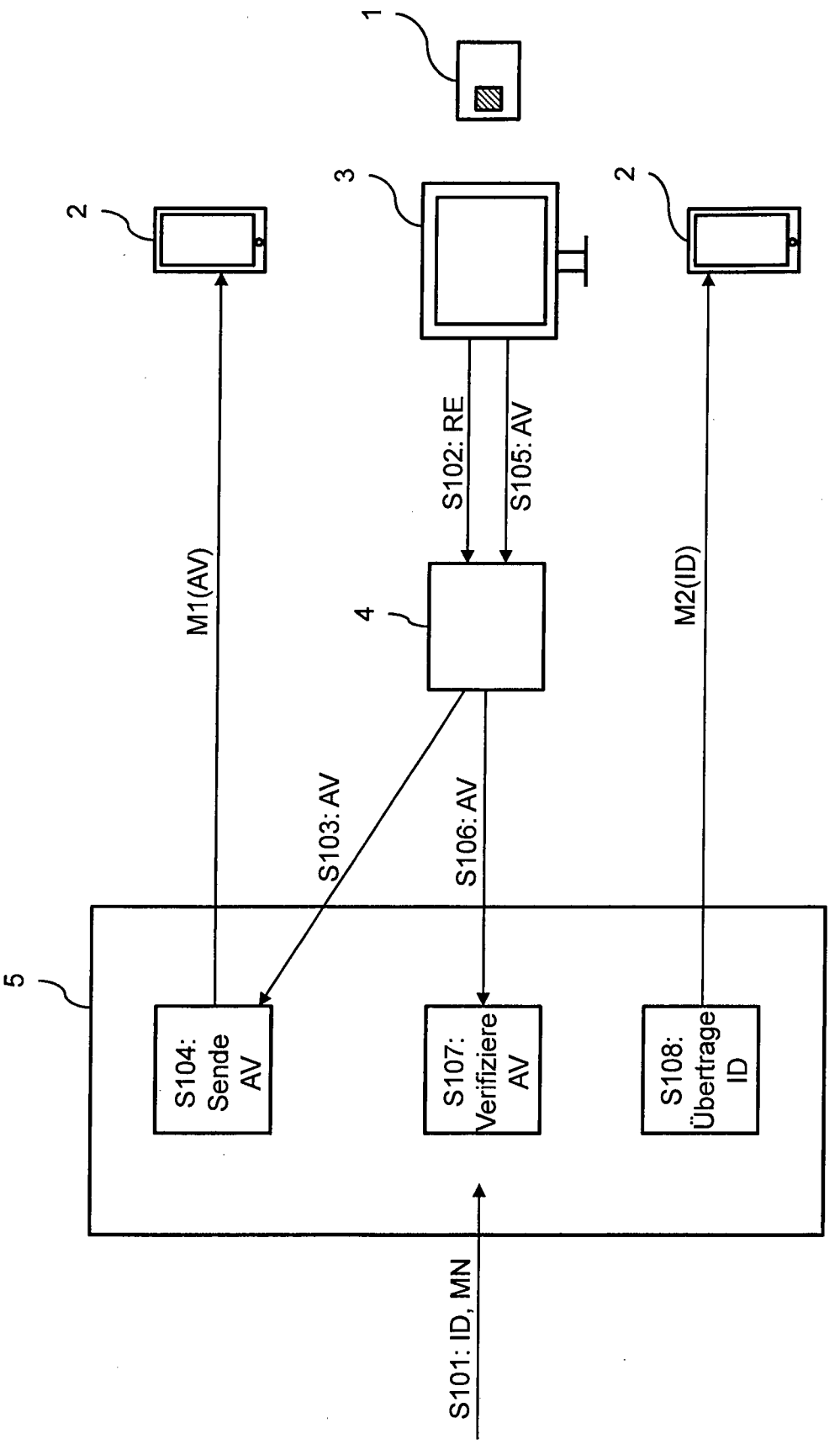
1
2
3
2
S102: RE
S105: AV
M1(AV)
M2(ID)
4
S103: AV
S106: AV
5
S104: Sende AV
S107: Verifiziere AV
S108: Übertrage ID
S101: ID, MN

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/000873

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L29/06
ADD. H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 528 045 A1 (WINCOR NIXDORF INT GMBH [DE]) 28 November 2012 (2012-11-28) abstract paragraph [0009] - paragraph [0027] paragraph [0030] - paragraph [0040]; figure 1 ----- -/--	1-15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2016	23/08/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Spranger, Stephanie

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "Transaction authentication number - Wikipedia, the free encyclopedia", , 13 March 2015 (2015-03-13), XP055198196, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Transaction_authentication_number&oldid=651206307 [retrieved on 2015-06-24] page 1, line 5 - page 2, line 12 page 2, line 40 - page 3, line 10 page 3, line 21 - page 4, line 26 -----	1-15
A	EP 2 187 363 A1 (OBERTHUR TECHNOLOGIES DENMARK [DK]) 19 May 2010 (2010-05-19) cited in the application abstract paragraph [0008] - paragraph [0025] paragraph [0050] - paragraph [0076]; figure 3 -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/000873

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2528045 A1	28-11-2012	DE 102011103292 A1	29-11-2012
		EP 2528045 A1	28-11-2012
		US 2012303527 A1	29-11-2012
EP 2187363 A1	19-05-2010	AT 553465 T	15-04-2012
		DK 2187363 T3	23-07-2012
		EP 2187363 A1	19-05-2010
		EP 2461297 A1	06-06-2012
		ES 2386259 T3	14-08-2012
		HR P20120575 T1	31-08-2012
		PT 2187363 E	16-07-2012
		SI 2187363 T1	28-09-2012
		US 2010332398 A1	30-12-2010

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2016/000873

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/08 H04L29/06
ADD. H04L9/32

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
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 UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 2 528 045 A1 (WINCOR NIXDORF INT GMBH [DE]) 28. November 2012 (2012-11-28) Zusammenfassung Absatz [0009] - Absatz [0027] Absatz [0030] - Absatz [0040]; Abbildung 1 ----- -/--	1-15

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen 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 internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen 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 Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
16. August 2016	23/08/2016

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Spranger, Stephanie

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	Anonymous: "Transaction authentication number - Wikipedia, the free encyclopedia", , 13. März 2015 (2015-03-13), XP055198196, Gefunden im Internet: URL:https://en.wikipedia.org/w/index.php?title=Transaction_authentication_number&oldid=651206307 [gefunden am 2015-06-24] Seite 1, Zeile 5 - Seite 2, Zeile 12 Seite 2, Zeile 40 - Seite 3, Zeile 10 Seite 3, Zeile 21 - Seite 4, Zeile 26 -----	1-15
A	EP 2 187 363 A1 (OBERTHUR TECHNOLOGIES DENMARK [DK]) 19. Mai 2010 (2010-05-19) in der Anmeldung erwähnt Zusammenfassung Absatz [0008] - Absatz [0025] Absatz [0050] - Absatz [0076]; Abbildung 3 -----	1-15

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2016/000873

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2528045 A1	28-11-2012	DE 102011103292 A1	29-11-2012
		EP 2528045 A1	28-11-2012
		US 2012303527 A1	29-11-2012
EP 2187363 A1	19-05-2010	AT 553465 T	15-04-2012
		DK 2187363 T3	23-07-2012
		EP 2187363 A1	19-05-2010
		EP 2461297 A1	06-06-2012
		ES 2386259 T3	14-08-2012
		HR P20120575 T1	31-08-2012
		PT 2187363 E	16-07-2012
		SI 2187363 T1	28-09-2012
		US 2010332398 A1	30-12-2010