WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/EP2019/073009**
International filing date:		**28 August 2019 (28.08.2019)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**DE**
	Number:	**20 2018 005 686.3**
	Filing date:	**30 November 2018 (30.11.2018)**
Date of receipt at the International Bureau:		**13 September 2019 (13.09.2019)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung
DE 20 2018 005 686.3
über die Einreichung einer Gebrauchsmusteranmeldung

Aktenzeichen:	20 2018 005 686.3
Anmeldetag:	30. November 2018
Anmelder/Inhaber:	Hoseit, Winrich, Dr., 50996 Köln, DE
Bezeichnung:	Elektronischer PIN-Safe
IPC:	G06F 21/34; G06K 19/07; G06F 21/60

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der Teile der am 30. November 2018 eingereichten Unterlagen dieser Gebrauchsmusteranmeldung unabhängig von gegebenenfalls durch das Kopierverfahren bedingten Farbabweichungen.

München, den 30. August 2019
Deutsches Patent- und Markenamt
Die Präsidentin
Im Auftrag

Götz

A 9161(Pat1)

30_11_2018-01-00005-00000009

„Elektronische PIN-Safe "

Diese Erfindung betrifft eine Vorrichtung zum kurzfristigen aber sicheren Auslesen von mehreren PIN`s (persönliche Identifikationsnummern) über nur eine einzige selbst vergebene alphanummerische Eingabefolge als Master PIN.

Heutzutage werden für viele Anwendungen Zugangscodes, also PIN`s für beispielsweise das Online-Banking, Bankkarten, Kreditkarten, Kundenzugänge, Rechnerzugang, Smartphone-Zugänge, Applikationszugänge, Internet- und Datenbankzugänge usw. vergeben. Die Vielzahl solcher PIN`s, Zugangs-Codes, Passwörter usw. sind für viele Anwender alleine aufgrund ihrer Vielzahl kaum im Gedächtnis zu behalten insbesondere erst recht nicht wenn sie seltener gebraucht werden.

Die Vertragspartner der Anwender, mit denen jeweils eine solche PIN vereinbart ist, schreiben aber in Ihren Nutzungsbedingungen zumeist vor, dass man diese PIN`s (Codes) an einem sicheren Ort verschlossen und vor dem Zugang durch Dritte sicher aufbewahren soll, sie nicht separat aufschreiben soll oder gar auf einem Zettel im Portemonnaie mitführen darf, ja man Gefahr läuft einen missbräuchlich verursachten Schaden nicht ersetzt zu bekommen, wenn die Sicherung dieser PIN nicht bedingungsgemäß vornimmt.

Die hier beschriebene Erfindung erlaubt es nun, alle PIN`s, Zugangscodes und Passwörter gesammelt so zu erfassen, dass Sie von Dritten nicht ausgelesen werden können aber dennoch im Zusammenspiel mit z.B. einem spezifischen Smartphone oder einem anderen spezifischen NFC-Auslesesystem dem Nutzer auf Abruf gesichert zur Verfügung stehen.

Die hier beschriebene Erfindung erlaubt es eine Vielzahl von unterschiedlichen PIN`s, Zugangscodes oder Passwörter mit nur einer einzigen selbst vergebenen Zahlen- oder Buchstabencodefolge aber auch in Verbindung oder nur mit einem Fingerabdruck sowie in weiterer Kombination mit oder nur mit einer Gesichtserkennung alleine oder beliebigen selbst gewählten Kombinationen daraus kurzzeitig unmittelbar vor dem Gebrauch dieser PIN`s, Zugangscodes

30_11_2018-01-00005-00000010

oder Passwörter abzurufen sofern die Authentifizierung sowohl über das diesem PIN-Safe gekoppelte Smartphone (Kamera, Fingerabdruck, Tastencode) oder ein sonstiges gekoppeltes Lesegerät zuvor erfolgt ist.

Der Träger dieser Informationen und der Abgleichprozesse kann erfindungsgemäß selbst z.B. die Größe einer Bankkarte haben aber auch eine sonstige Vorrichtung oder auch ein sogenanntes „Wearable" sein und kann dauerhaft ohne eine eigene Stromquelle auskommen.

Die hier vorgestellte Erfindung beschreibt erfindungsgemäß z.B. eine Plastikkarte in Form einer Bankkarte in der ein NFC-Chip mit einem programmierbaren Controller und Speicher integriert ist.

Nach dem Stand der Technik sind passive NFC-Chips bekannt die ohne eine eigene Stromversorgung auskommen aus einem Mikrochip, einem Kondensator und einer Antenne meist in Form einer Metallspule bestehen. Hinzu kommt bei beschreibbaren Varianten ein Speicher von derzeit bis zu vier Megabyte Größe.

Erfindungsgemäß wird dieser Vorrichtungs- bzw. Karten-Speicher über eine Schnittstelle zu einem Smartphone oder Computer erstmals so programmiert, dass er nach Abschluss der ersten Programmierung nur wieder über eine selbst vergebene PUK, auch in Verbindung mit dem Abgleich eines Finderabdrucks oder dem Gesichtsabgleich des für diese Vorrichtung/Karte erstmals gekoppelten Smartphone bzw. den erstmals gekoppelten Computer angesprochen, geöffnet und re-programmiert werden kann.

Die erste Programmierung der hier beschriebenen Vorrichtung (PIN-Safe-Karte) erfordert außer der PUK-Eingabe erfindungsgemäß z.B. auch die IMSI sowie die MAC-Adresse des Smartphones oder eine andere gerätespezifische Identifikationsnummer oder Kombination des erstmals angebundenen Rechnersystems bzw. der angebundenen und gekoppelten Rechnersysteme (Smartphone / Computer) daraus als auch eine Liste all der PIN`s, Zugangscodes und Passwörter zu denen man einen gesicherten Zugang über sein initial gekoppeltes Smartphone oder sonstiges authentifiziertes Abrufgerät herstellen möchte.

30_11_2018-01-00005-00000011

Unter PIN oder PIN`s werden hier erfindungsgemäß auch sonstige Zugangscodes und Passwörter und sonstige Kombinationen aus diesen sowie anderen numerischen oder alphanumerischen Codes oder Kombinationen daraus verstanden.

Als NFC-Lesegeräte wird erfindungsgemäß ein Smartphone gewählt, dessen IMSI als auch MAC-Adresse oder eine andere gerätespezifische Identifikationsnummer oder Kombination daraus über eine zu dieser Vorrichtung gehörende App abgeglichen wird, so dass erfindungsgemäß nur dann am Display des Smartphones die Liste der vertraulichen PIN`s angezeigt werden, wenn dieses Lesegerät die Ausgabe „anfordert" und im Smartphone vor dem Anzeigen auch die PUK eingegeben wurde.

NFC Systeme – wie sie heute in den meisten Smartphones verwendet werden, erzeugen ein elektromagnetisches (13,56-MHz) Wechselfeld wenn man den erfindungsgemäß wie hier beschrieben programmierten passiven Chip wie er in der der hier beschriebenen Vorrichtung (Karte) enthalten ist, in dessen unmittelbare Nähe hält. Die Antenne der in dieser Erfindung befindlichen NFC-Einheit nimmt die Hochfrequenzenergie der NFC-Sendeeinheit des Smartphones auf, puffert diese Energie in einem z.B. Kondensator und versorgt den in der Karte befindlichen Mikrochip mit Strom um den Abgleich mit dem aufrufenden Smartphone vorzunehmen und die Daten dann zum Smartphone zu übertragen, wenn die Sicherheitsabfragen alle erfolgreich beantwortet wurden.

Diese Spulenanregung reicht durch die NFC-Vorrichtung im Smartphone reicht aus, um Daten wie die Chip-Seriennummer (ID), Systembefehle, Text und kleine Bilder zu übertragen, zu lesen und auszutauschen.

Die Programmierung kann erfindungsgemäß aber auch über eine andere autorisierte NFC-Vorrichtung, also auch das Smartphone erfolgen. Die gesicherten PIN`s können ergänzt werden durch Informationen, die dann auch zusammen mit der PIN angezeigt werden, wie z.B.

30_11_2018-01-00005-00000012

Master Card-Bargeldabhebung: 40934
Volksbank-Online Banking: Zugangscode 0815
Passwort 4711
Commerzbank Köln: 45672
1&1-Web-Hosting: Zugangscode: w.muster@man.de
Passwort: Zigeuner

usw.

Die Programmierung der hier beschriebenen Vorrichtung kann erfindungsgemäß auch über eine Kontaktfläche oder Steckverbindung erfolgen.

Nach dem Stand der Technik sind RFID-Lösungen und NFC-Lösungen bekannt, die sowohl Lese- als auch Schreibvorgänge von Dateninhalten und entsprechende Autorisierungsprüfungen vor der Datenausgabe vornehmen können.
In Erweiterung solcher Autorisierungsprüfungen werden hier erfindungsgemäß einmalige Gerätekennungen in Verbindung mit einem Mastercode (PUK) als auch Master-PIN zum auslesen besonders geschützter Dateninhalte verwendet.

Dieser Erfindung liegt daher die Aufgabe zugrunde, ganz besonders sensible und werthaltige Daten, wie insbesondere PIN`s, Zugangscodes und Passwörter mehrerer anderer Geräte oder Applikationen in einer erfindungsgemäß hier beschriebenen Vorrichtung / Karte durch das Auslesen mehrerer hintereinander geschalteter Prüfparameter (Master-PIN, MAC-Adresse des Lesegerätes, IMSI des im Smartphone befindlichen Chips des Mobilfunkproviders, Fingerabdruck, Gesicht) in einer beliebigen Reihenfolge so zu kombinieren, wie es das Sicherheitsbedürfnis des Nutzers vorgibt.

Dieser Erfindung liegt weiterhin die Aufgabe die Nutzung, also das Aufzeigen von sensiblen Daten zwar skalierbar mit einem hohen selbst einstellbaren Sicherheitsgrad für Dritte nahezu unmöglich einsehbar zu machen aber von der Handhabung für den Nutzer dennoch so einfach wie möglich zu gestalten.

Das hier beschriebene System besteht z.B. aus folgenden Bauteilen:
Die hier beschriebene Speicher-Vorrichtung (1) in Form z.B. einer Plastik-Bank-

30_11_2018-01-00005-00000013

oder Kreditkarte weist Bauelemente auf wie eine (NFC) Induktionsspule zur Aufnahme der Sendeenergie des Lesegerätes (9), einem Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller (3) zur bidirektionalen Kommunikation mit dem Lesegerät (9) z.B. einem Smartphone, als auch einen Datenspeicher (4) in dem die besonders zu schützenden Dateninhalte wie PIN`s, Zugangscodes und Passwörter, sowie deren Bezeichnung, wofür diese Verwendung finden, auch verschlüsselt abgelegt sind.

Weiterhin besteht das System aus einem Lesegerät (9) mit je einer eindeutigen Geräteadresse (MAC-Adresse) als auch einer einmaligen IMSI-Kennung, das ebenfalls eine (NFC) Spule (2) zur bidirektionalen Kommunikation aufweist. Weiterhin enthält dieses Lesegerät (9) über eine eigene Applikation gesteuert und aufgerufen, ein Tastaturfeld (6) zur Eingabe der Master-Pin, bzw. der Master PUK bereit als auch ein Display (5) zur Anzeige der im Speicher (4) verschlüsselt abgelegten Dateninhalte, die erst angezeigt werden, wenn alle individuell skalierbar eingestellten Prüfwerte übereinstimmen, insbesondere die Authentifizierung über die im Tastenfeld (6) eingegebene Master-Pin auch in Verbindung mit dem als richtig erkannten Fingerabdruck, eingeben über den Fingerabdrucksensor (8) aber auch in Verbindung mit dem über die Kamera (7) als richtig erkannte Gesichtsform frei gegeben wurde.

Mit der dieser Erfindung zugrunde liegenden Funktionen werden mit entweder nur einem Master-Pin mehrere andere PIN`s, Zugangscodes und Passwörter auf einem gekoppelten Lesegerät(Smartphone) angezeigt wobei es dem Nutzer überlassen bleibt, diese Master-Pin selbst zu generieren aber auch von weiteren Prüfkriterien abhängig machen kann, wie Fingerabdruck und Gesichtserkennung unter Umständen auch sogar über eine Spracherkennung auch von Schlüsselwörtern.

Es gibt nun eine Vielzahl von Möglichkeiten die Erfindung auszugestalten und weiterzubilden. Hierfür darf auf die dem Schutzanspruch 1 nachgeordneten Schutzansprüche verwiesen werden.
Eine bevorzugte Ausgestaltung wird nun anhand der Zeichnung und der dazugehörigen Beschreibung beispielhaft näher erläutert.

30_11_2018-01-00005-00000014

Bezugszeichenliste:

1	Trägereinheit (Karte) der Vertraulichen Informationen (PIN, Zugangscode, Passwort usw.)
2	NFC-Spule
3	Controller-Chip
4	Speicher (Chip) der vertraulichen Informationen
5	Display des Auslesegerätes (Smartphone)
6	Eingabetastatur des Auslesegerätes (Smartphone)
7	Kamera des Auslesegerätes (Smartphone)
8	Fingerabdruckleser
9	gekoppeltes Auslesegerät (Smartphone)

30_11_2018-01-00005-00000015

Begriffsbestimmungen:

PIN	= persönliche Identifikationsnummer
PUK	= personal unblocking key
NFC	= Near Field Communication
IMSI	= International Mobile Subscriber Identity
MAC- Adresse	= Media Access Controll Adresse (Hardware ID)
ID	= Identifikations-Kennung
RFID	= Radio Frequency Identification

30_11_2018-01-00005-00000016

In der Zeichnung zeigt:

Fig. 1 eine schematischen Darstellung des Trägers der vertraulichen Informationen (PIN, Zugangscode, Passwort usw.)

Fig. 2 eine schematischen Darstellung des gekoppelten Programmier- und Auslesegerätes der vertraulichen Informationen (Smartphone) mit der dazugehörigen Software (Applikation) zur Verwaltung der Sicherheitsstufen als auch der zu schützenden Dateninhalte.

30_11_2018-01-00005-00000018

Schutzansprüche:

1. NFC-Kommunikationssystem, bestehend aus einer Trägereinheit (Chip-Karte), **dadurch gekennzeichnet**, dass diese vertrauliche Informationen, insbesondere PIN`s, Zugangscodes, Passwörter enthält, die nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmiereinheit (Smartphone mit IMEI-Adresse) und / oder der gerätespezifischen MAC-Adresse) unter Eingabe oder Abruf einzelner oder mehrerer vordefinierter Informationen der Authentifizierung, wie frei vom Nutzer programmierbare und skalierbare alphanumerische Codes, Fingerabdrücke, Gesichtserkennung, Spracherkennung u.ä. wieder abgerufen bzw. geändert oder gelöscht werden können.

2. NFC-Kommunikationssystem, bestehend aus einer Trägereinheit (Chip-Karte), **dadurch gekennzeichnet**, dass diese vertrauliche Informationen wie PIN`s, Zugangscodes, Passwörter enthält, deren Abruf einzeln unterschiedlich nach beliebig skalierbaren Authorisierungsabfragen, wie einer Master-Pin, einem Fingerabdruck, einem erkannten Gesicht oder einer Sprachsequenz möglich ist.

3. NFC-Kommunikationssystem, bestehend aus einer Lese- und Programmiereinheit (Smartphone / Rechner) , **dadurch gekennzeichnet**, dass diese gekoppelt an die im Schutzanspruch 1 beschriebene Trägereinheit unter Eingabe einer Master-PIN die in der Trägereinheit befindlichen vertraulichen Informationen abruft und anzeigt, sofern alle Authentifizierungsanforderungen der Trägereinheit erfüllt sind.

4. NFC-Kommunikationssystem, bestehend aus einer Lese- und Programmiereinheit (Smartphone / Rechner) , **dadurch gekennzeichnet**, dass diese gekoppelt an die im Schutzanspruch 1 beschriebene Trägereinheit unter Eingabe einer Master-PIN, eines als richtig erkannten Fingerabdrucks, eines als richtig erkannten Gesichts, eines als richtig erkannten Sprachinhaltes oder der Sprache an sich oder diese einzeln oder in einer beliebigen Kombination vom Nutzer festgelegten Reihenfolge skaliert, die in der Trägereinheit befindlichen vertraulichen Informationen abruft und anzeigt.

30_11_2018-01-00005-00000019

5. NFC-Trägereinheit, **dadurch gekennzeichnet**, dass diese bei mehrfach falscher Authentifizierungseingabe den weiteren Abruf der vertraulichen Informationen befristet oder vollständig sperrt und nur gegen eine vom Nutzer selbst vergebene übergeordnete PUK wieder zu reaktivieren ist.

6. NFC-Trägereinheit, **dadurch gekennzeichnet**, daß diese in Form einer Bank- oder Kreditkarte ausgestaltet auch als Werbeträger verwendet werden kann.

7. NFC-Trägereinheit, **dadurch gekennzeichnet**, dass diese selbst eine funktionsfähige Bankkarte oder Kreditkarte ist auf der diese Art des Auslesens mehrerer PIN`s mit einem autorisiert gekoppelten Lesegerät möglich ist.

30_11_2018-01-00005-00000007

Zusammenfassung:

Der hier beschriebene elektronische PIN-Safe als Bankkarte erlaubt es einzelne oder eine Liste mehrerer PIN`s, Zugangscodes oder Passwörter oder sonstige vertrauliche Inhalte mittels eines für ein gekoppeltes Smartphones mit der Eingabe nur eines einzigen vom Nutzer selbst gestalteten Master-PIN`s auszulesen, macht es aber auch möglich die Prüftiefe insgesamt oder für einzelne vertraulich abgespeicherte Inhalte durch das Abprüfen des Fingerabdrucks, des Gesichtes des Nutzers und über die Eingabe einer Sprachsequenz zu erhöhen.

30_11_2018-01-00005-00000021

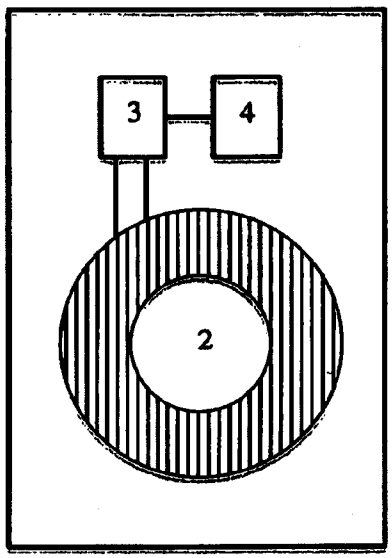

Fig.1

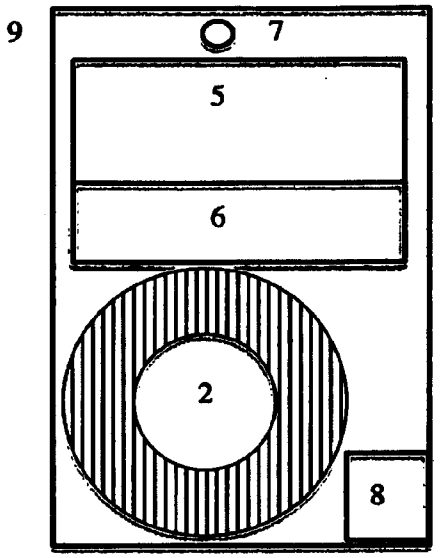

Fig.2