

NFC-Kommunikationssystem und NFC-Trägereinheit

Diese Erfindung betrifft ein NFC-Kommunikationssystem und eine NFC-Trägereinheit. Die NFC Trägereinheit dient 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.

Aus der WO2019/020824 A1 ist eine Smart-Card mit integriertem Prozessor zur Verschlüsselung bekannt. In einem Speicher der Karte ist ein Teil eines privaten Schlüssels gespeichert, der mit einem lokal gespeicherten separaten Schlüssel für die digitale Signatur von Transaktionen von Kryptowährung verwendbar ist. Durch die Smart-Card mit Krypto-Prozessor können Anfragen an die Karte gestellt werden, um mit einem Zugriffspasswort den enthaltenen Teil des Privaten Schlüssels zu erhalten. Kryptographieoperationen laufen auf der SmartCard. Diese kann von jedem Smart-Card Lesegerät genutzt werden, sofern die zweite Hälfte des Schlüssels vorhanden ist. Auf der Smart-Card ist nur der halbe Schlüssel gespeichert, der Speicher kann

von jedem Smart-Card Lesegerät gelesen werden. Für weitere Verwendung wird die zweite Schlüsselhälfte benötigt.

Der Erfindung liegt die Aufgabe zu Grunde, das NFC-Kommunikationssystem und eine NFC-Trägereinheit zu verbessern.

Die Aufgabe wird nun durch ein NFC-Kommunikationssystem und eine NFC-Trägereinheit gemäß der unabhängigen Patentansprüche gelöst.

Das erfindungsgemäße NFC-Kommunikationssystem weist eine Trägereinheit, insbesondere in Form einer Chip-Karte auf, wobei die Trägereinheit eine NFC-Induktionsspule zur Aufnahme der Sendeenergie eines Lesegerätes, einen Controller, einen Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller zur bidirektionalen Kommunikation mit dem Lesegerät sowie einen Speicher mit vertrauliche Informationen, insbesondere PIN's, ZugangsCodes, Passwörter enthält, wobei die vertraulichen Informationen nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmierereinheit, insbesondere ein Smartphone mit einer 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.

Die erfindungsgemäße NFC-Trägereinheit weist eine NFC-Induktionsspule zur Aufnahme der Sendeenergie eines Lesegerätes, einen Controller, einen Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller zur bidirektionalen Kommunikation mit dem Lesegerät sowie einen Speicher mit vertrauliche Informationen, insbesondere PIN's, ZugangsCodes, Passwörter auf, wobei die vertraulichen Informationen nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmierereinheit, insbesondere ein Smartphone mit einer 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. Die NFC-Trägereinheit wird im folgenden auch als Karte, Pin-Safe Karte bezeichnet.

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 NFC –Trägereinheit enthält im Speicher vertrauliche Informationen wie PIN's, Zugangscodes, Passwörter, deren Abruf einzeln unterschiedlich nach beliebig skalierbaren Authorisierungsabfragen, wie einer Master-Pin, einem Fingerabdruck, einem erkannten Gesicht oder einer Sprachsequenz möglich ist.

Die Lese- und Programmierereinheit wird an die Trägereinheit gekoppelt unter Eingabe einer Master-PIN und ruft dann die in der Trägereinheit befindlichen vertraulichen Informationen ab und zeigt die Informationen, sofern alle Authentifizierungsanforderungen der Trägereinheit erfüllt sind.

Die Lese- und Programmierereinheit insbesondere ein Smartphone oder ein Rechner, wird an die Trägereinheit gekoppelt 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 unter Eingabe dieser Merkmale einzeln oder in einer beliebigen Kombination vom Nutzer festgelegten Reihenfolge skaliert, wobei Lese- und Programmierereinheit die in der Trägereinheit befindlichen vertraulichen Informationen abrufen und anzeigt.

Eine IMSI und/oder MAC-Adresse oder eine andere gerätespezifische Identifikationsnummer des Leseegerätes, insbesondere des Smartphones, oder Kombination daraus wird/werden über eine zu dem Leseegerät gehörende App abgeglichen, so dass nur dann am Display des Leseegerätes die Liste der vertraulichen PIN's angezeigt werden, wenn dieses Leseegerät die Ausgabe „anfordert“ und im Leseegerät vor dem Anzeigen auch die PUK eingegeben wurde.

Die Trägereinheit sperrt bei mehrfach falscher Authentifizierungseingabe den weiteren Abruf der vertraulichen Informationen befristet oder vollständig und ist nur gegen eine vom Nutzer selbst vergebene übergeordnete PUK wieder zu reaktivieren ist.

Die NFC-Trägereinheit kann in Form einer Bank- oder Kreditkarte ausgestaltet sein und kann vorzugsweise auch als Werbeträger verwendet werden. Die NFC-Trägereinheit kann selbst eine funktionsfähige Bankkarte oder Kreditkarte sein, auf der diese Art des Auslesens mehrerer PIN's mit einem autorisiert gekoppelten Lesegerät möglich ist.

Die hier beschriebene Erfindung erlaubt es eine Vielzahl von unterschiedlichen PIN's, Zugangscodes oder Passwörter mit nur einer einzigen selbst vergebenen Zahlen- oder Buchstabencodedefolge 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 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 vorzugsweise z.B. eine (Plastik-)Karte 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.

Insbesondere wird dieser Vorrichtung- 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 Fingerprintabdrucks oder dem Gesichtsabgleich des für diese Vorrichtung/Karte erstmals gekoppelten Smartphone bzw. den erstmals gekoppelten Computer angesprochen, geöffnet und reprogrammiert werden kann.

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

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 und/oder MAC-Adresse oder eine andere gerätespezifische Identifikationsnummer oder Kombination daraus über eine zu dem Lesegerät 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 hier beschriebenen Trägereinheit (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 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. 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 insbesondere 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 vorzugsweise einmalige Gerätekennungen in Verbindung mit einem Mastercode (PUK) als auch Master-PIN zum Auslesen besonders geschützter Dateninhalte verwendet.

Dieser Erfindung hat den Vorteil, dass ganz besonders sensible und werthaltige Daten, wie insbesondere PIN's, Zugangscode 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 kombinierbar sind, wie es das Sicherheitsbedürfnis des Nutzers vorgibt.

Dieser Erfindung hat ferner den Vorteil, dass also das Aufzeigen von sensiblen Daten zwar skalierbar mit einem hohen selbst einstellbaren Sicherheitsgrad für Dritte nahezu unmöglich einsehbar zu machen ist, aber von der Handhabung für den Nutzer dennoch so einfach wie möglich gestaltet ist. Das hier beschriebene System besteht z.B. aus folgenden Bauteilen:

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. 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.

Die hier beschriebene Speicher-Vorrichtung 1 in Form z.B. einer Plastik-Bank- oder Kreditkarte weist Bauelemente auf wie eine (NFC) Induktionsspule zur Aufnahme der Sendeenergie des Lesegerätes 9, einen 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, Zugangscode 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.

Bei der ersten Verwendung der PINSAFE-Karte (1) wird die PIN-SAFE App auf dem Lesegerät (9) bzw. Smartphone installiert. Nach der Installation wird die PINSAFE-Karte unter das Smartphone gelegt. Im Kopplungsprozess wird eine selbstgewählte Master-PIN vergeben. Jetzt können beispielsweise bis zu 50 vertrauliche Kurzdaten im Chip-Tresor der PINSAFE Karte verwaltet werden.

Die PIN-SAFE-App erlaubt die Sicherheitsstufe noch erheblich weiter hoch zu erhöhen:

- Gesichtserkennung
- Fingerabdruck
- Spracherkennung

können zukünftig in frei gewählter Abfolge vor dem Anzeigen der vertraulichen Daten genutzt werden.

Eine weitere PIN-SAFE-Karte (1) kann als Sicherung erstellt werden.

Die Kombination der Benutzer-PIN mit der weltweit einmaligen ID des Gerätes (IMEI: *#06#) und einer Zufallszahl generiert einen Schlüssel, der für höchste Sicherheit sorgt.

PIN-SAFE-Karte (1) ist ein Offline-Datenspeicher. Die Daten befinden sich physisch auf der PIN-SAFE-Karte. Nur gekoppelt mit der IMEI jeweils eines einzigen Smartphones (9) unter Eingabe einer selbst generierten Master-Pin werden vertrauliche Kurzdaten auf nur dieser einen PIN-SAFE-Karte bzw. einer Backup-Karte gespeichert und nur auf dem Display (5) des einen Smartphones (9) des einen Nutzers angezeigt und zwar auch nur dann, wenn die PIN-SAFE-Karte unter das gekoppelte Smartphone gehalten wird.

Die PIN-SAFE-Karte (1) erfüllt als NFC-OFFLINE Datenspeicher die Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI-Richtlinie: TR-02102-1). Die Verwaltung der vertraulichen und persönlichen Kurzdaten erfolgt über die kostenlos erhältliche PIN-SAFE-APP. Voraussetzung ist ein NFC-fähiges Smartphone (9). Eine IOS-Lösung für APPLE Smartphones ist möglich. Solange APPLE das Beschreiben von NFC-Karten noch nicht erlaubt, wird die IOS-PIN-SAFE-Karte mit einem USB-/BlueTooth-Schreibgerät ausgeliefert; das Lesen der Daten geht schon heute.

Die PIN-SAFE-Karte(1) hat einen Gesamtspeicher von 868 Byte und kann nach ihrer Codierung mit netto 800 Byte ca. 50 vertrauliche Geheimzahlen und Passwörter und ihre dazugehörigen Namensbezeichnungen (durchschnittlich je 16 Byte) speichern; über die PINSAFE-APP werden diese Daten bequem und übersichtlich angezeigt und verwaltet.

Während der Bearbeitung sind alle Daten für die Dauer, die die PIN-SAFE-APP aktiv ist, sichtbar und werden auch nur solange befristet im flüchtigen Speicher des Smartphones angezeigt wie die PIN-SAFE-APP geöffnet ist. Die Daten-Speicherung erfolgt ausschließlich und nur verschlüsselt auf der PIN-SAFE-Karte; die APP fordert zum Ankoppeln der Karte auf.

Die Verschlüsselung erfolgt über eine 3-Faktor AES256-Codierung. Veranschaulicht heißt das: Wenn alle Bewohner der Erde, ausgestattet mit je 1.000 Computern, die je 1 Mio. Daten pro Sek. analysieren können, versuchen wollten die o.g. Codierung zu entschlüsseln, würden die nächsten 4,5 Milliarden Jahre (vermutete Restlaufzeit der Erde) nicht ausreichen auch nur die Hälfte dieser Verkryptung zu decodieren.

Die PIN-SAFE Karte (1) hat bewusst das Format einer Bankkarte und passt somit ideal ins Portemonnaie in dem auch üblicherweise die Bank- und Kreditkarten stecken. Am Bankautomat oder vor dem PC legt der Nutzer die PIN-SAFE-Karte nur unter sein gekoppeltes Smartphone (9) und nach Eingabe der selbst erstellten PIN-SAFE-PIN erscheinen alle vertraulichen Kurzdaten nur im Display dieses einen Smartphones. Eine Schutzhülle für die Karte ist nicht erforderlich.

Gegen den Verlust der PIN-SAFE-Karte (1) hilft eine Back-Up-Kopie; diese Kopie kann offen aufbewahrt werden, da sie nicht von Dritten ohne das gekoppelte Smartphone (9) und ohne den selbst erstellten und dazugehörigen PIN ausgelesen werden kann.

Sollte der Nutzer sein Smartphone wechseln kann die PIN-SAFE-Karte (1) auf das neue Smartphone (9) mit der IMEI des alten Smartphones (9) innerhalb eines definierten Zeitfensters zu der neuen IMEI des neuen Smartphones (9) übertragen werden. Hierzu ist wieder die selbst vergebene PIN erforderlich.

Beim gleichzeitigen Verlust von Smartphone (9) und Portemonnaie schützt als letzte Hürde immer noch die vom Nutzer selbst generierte PIN-SAFE-PIN vor einem Missbrauch.

Anstatt also die Daten einem Zettel oder einem Programm-Speicher, der ONLINE angesprochen werden kann, anzuvertrauen schützt der PIN-SAFE-OFFLINE-Speicher nicht nur dadurch, dass er eben OFFLINE ist sondern auch dadurch, dass die Daten nur mit dem vom Nutzer gekoppelten Smartphone (9) in einem kurzen Zeitfenster mit der individuellen PIN sichtbar sind.

Bezugszeichenliste

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

Begriffsbestimmungen:

PIN = persönliche Identifikationsnummer

PUK = personal unblocking key NFC = Near Field Communication

IMSI = International Mobile Subscriber Identity

MAC- Adresse = Media Access Control Adresse (Hardware ID) ID = Identifikations-Kennung

RFID = Radio Frequency Identification

Patentansprüche

1. NFC-Kommunikationssystem, mit einer Trägereinheit (1), insbesondere in Form einer Chip-Karte, wobei die Trägereinheit (1) eine (NFC) Induktionsspule (2) zur Aufnahme der Sendeenergie eines Lesegerätes (9), einen Controller (3), einen Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller (3) zur bidirektionalen Kommunikation mit dem Lesegerät (9) sowie einen Speicher (4) mit vertrauliche Informationen, insbesondere PIN's, Zugangscodes, Passwörter enthält, wobei die vertraulichen Informationen nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmierereinheit (9), insbesondere ein Smartphone mit einer 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, mit einer Trägereinheit (1) nach Anspruch 1, 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, mit einer Lese- und Programmierereinheit (9), insbesondere einem Smartphone und/oder einem Rechner, dadurch gekennzeichnet, dass die Lese- und Programmierereinheit (9) gekoppelt an die Trägereinheit (1) unter Eingabe einer Master-PIN die in der Trägereinheit (1) befindlichen vertraulichen Informationen abrufen und anzeigt, sofern alle Authentifizierungsanforderungen der Trägereinheit (1) erfüllt sind.

4. NFC-Kommunikationssystem, mit einer Lese- und Programmierereinheit (9) (Smartphone / Rechner), dadurch gekennzeichnet, dass diese gekoppelt an die Trägereinheit (1) 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 (1) befindlichen vertraulichen Informationen abrufen und anzeigen.

4. NFC-Kommunikationssystem, mit einer Lese- und Programmierereinheit (9) (Smartphone / Rechner), dadurch gekennzeichnet, dass eine IMSI und/oder MAC-Adresse oder eine andere gerätespezifische Identifikationsnummer des Leseegerätes (9), insbesondere des Smartphones, oder Kombination daraus über eine zu dem Leseegerät (9) gehörende App abgeglichen wird, so dass nur dann am Display des Leseegerätes die Liste der vertraulichen PIN's angezeigt werden, wenn dieses Leseegerät (9) die Ausgabe „anfordert“ und im Leseegerät (9) vor dem Anzeigen auch die PUK eingegeben wurde.

5. NFC-Trägereinheit (1), wobei die Trägereinheit (1) eine (NFC) Induktionsspule (2) zur Aufnahme der Sendeenergie eines Leseegerätes (9), einen Controller (3), einen Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller (3) zur bidirektionalen Kommunikation mit dem Leseegerät (9) sowie einen Speicher (4) mit vertraulichen Informationen, insbesondere PIN's, Zugangscodes, Passwörter enthält, wobei die vertraulichen Informationen nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmierereinheit (9), insbesondere ein Smartphone mit einer 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.

6. NFC-Trägereinheit (1) nach dem vorstehenden Anspruch, dadurch gekennzeichnet, dass die Trägereinheit (1) 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.

7. NFC-Trägereinheit (1) nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die NFC-Trägereinheit (1) in Form einer Bank- oder Kreditkarte ausgestaltet ist und vorzugsweise auch als Werbeträger verwendet werden kann.

8. NFC-Trägereinheit (1) nach einem der vorstehenden Ansprüche, 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 (9) möglich ist.

Zusammenfassung:

NFC-Kommunikationssystem und NFC-Trägereinheit

Die Erfindung betrifft ein NFC-Kommunikationssystem, mit einer Trägereinheit (1), insbesondere in Form einer Chip-Karte, wobei die Trägereinheit (1) eine (NFC) Induktionsspule (2) zur Aufnahme der Sendeenergie eines Lesegerätes (9), einen Controller (3), einen Kondensator zur Speicherung und Abgabe der aufgenommenen Energie an den Controller (3) zur bidirektionalen Kommunikation mit dem Lesegerät (9) sowie einen Speicher (4) mit vertrauliche Informationen, insbesondere PIN's, Zugangscodes, Passwörter enthält, wobei die vertraulichen Informationen nur über eine zu ihr eindeutig gekoppelte Lese- bzw. Programmiereinheit (9), insbesondere ein Smartphone mit einer 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.

Fig. 1

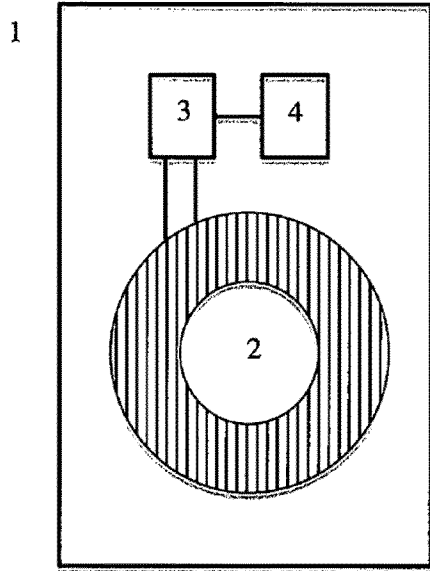


Fig.1

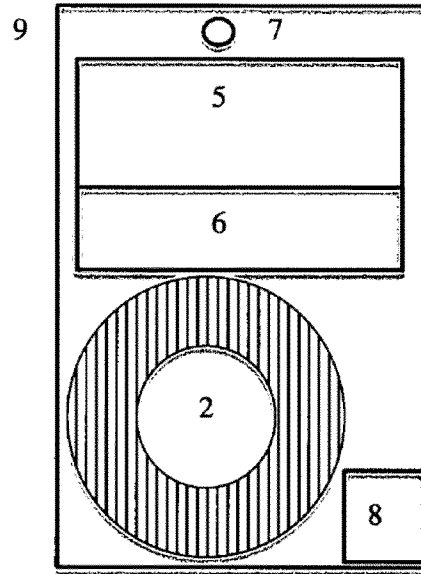


Fig.2