

# Alternativer elektronischer Personalausweis

(Ernst Erich Schnoor)

Der **neue elektronische Personalausweis** kann ab dem 1. November 2010 von jedem Bundesbürger beantragt und angewendet werden. Aufgabe des neuen Ausweises ist „die herkömmliche Nutzung von Ausweisen in die digitale Welt zu übertragen und sich im Internet eindeutig auszuweisen“ ([www.ausweisapp.bund.de/...](http://www.ausweisapp.bund.de/)). Erste Erfahrungen im Umgang mit dem neuen Personalausweis zeigen, dass das Verfahren etwas umständlich, schwer zu handhaben und noch mit Schwachstellen behaftet ist.

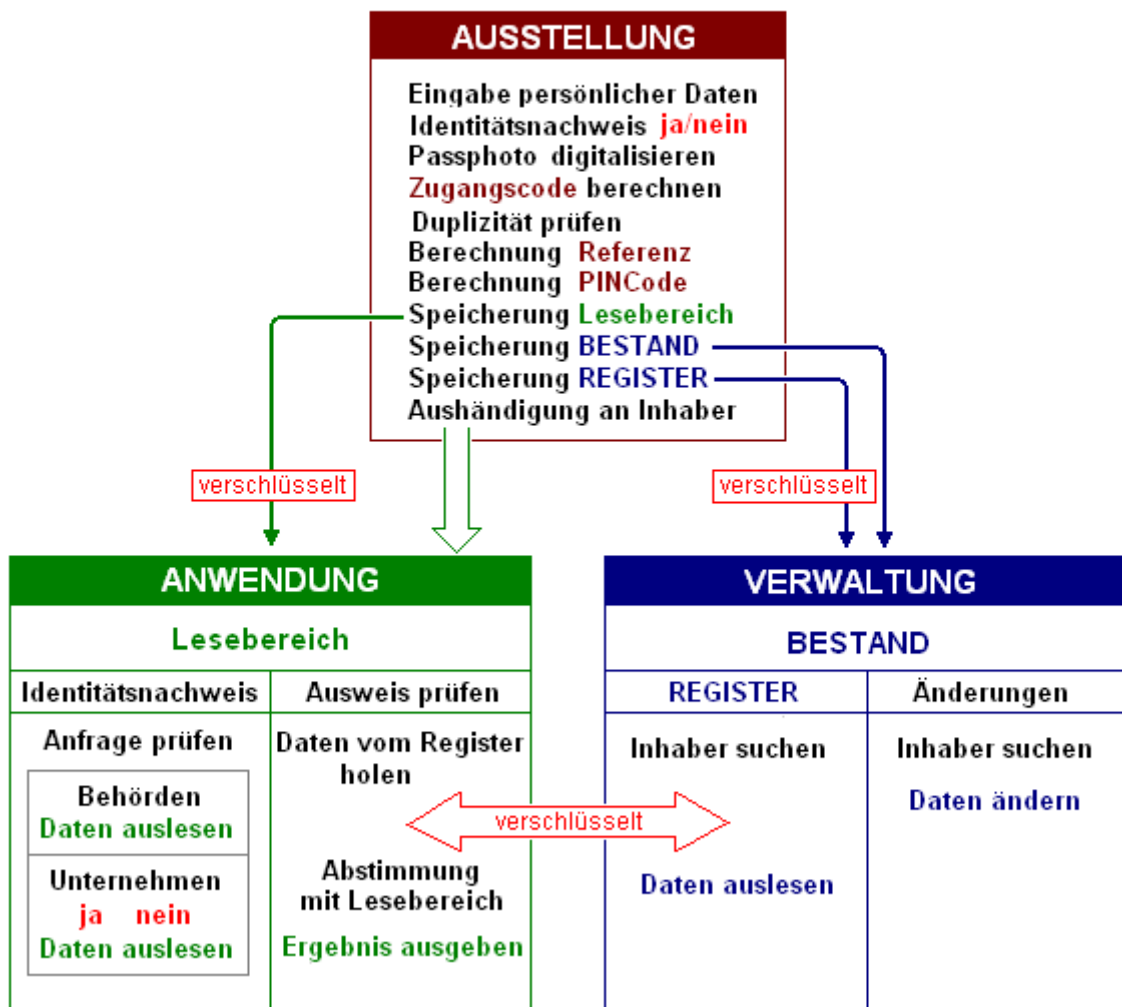
Aber, es geht auch einfacher und mit wesentlich geringerem Aufwand. Als Alternative bietet sich eine Lösung an mit dem vom Autor entwickelten **CypherMatrix** Verfahren. Die Grundlagen des Verfahrens werden ausführlich erläutert in den folgenden Artikeln:

<http://www.telecypher.net/Bytetechnik.pdf>

<http://www.telecypher.net/Basisfunktion.pdf>

Die Zusammenhänge des alternativen Personalausweises stellen sich wie folgt dar:

## elektronischer Personalausweis



Es handelt sich um ein völlig neues Verfahren. Daher könnte das Verstehen der Zusammenhänge und Abläufe mit herkömmlichen Vorstellungen etwas ungewohnt sein (keine vertrauten Abläufe in traditioneller **Bittechnik** sondern nur **Bytetechnik** und einfache Mathematik). Das zum Testen des Verfahrens geschriebene Programm bietet folgendes Menü:

## Menue

Ausstellung

Anwendung

Verwaltung

Beenden

### A. Ausstellung des Personalausweises

Zur Erläuterung der Abläufe wird ein Beispiel gewählt mit erfundenen Daten, die in keinem Zusammenhang mit realen Personen stehen. Die Ausstellungsbehörde erstellt den Ausweis in folgenden Schritten:

#### a) Eingabe der persönlichen Daten des Antragstellers

1. Familienname und Geburtsname: **Berger**
2. Rufname (Vorname): **Karl**
3. weitere Vornamen: **Friedrich Wilhelm**
4. Tag der Geburt: **14.07.1952**
5. Ort der Geburt: **Großkarolinenfeld**
6. Geburtsname der Mutter: **Soltwedel**
7. Wohnort des Antragstellers: **Berlin**
8. Anschrift des Antragstellers: **Lützowplatz 37**
9. Doktorgrad (ja/nein):
10. Staatsangehörigkeit: **deutsch**
11. Ordensname, Künstlername:
12. Gültigkeitsdauer: **gültig bis 31.12.2020**
13. Identitätsnachweis (ja/nein): **ja**
14. Sperrvermerke: **keine Vermerke**

Die Daten **1** bis **7** und **9** bis **11** werden zusammengefasst und mit der **CypherMatrix** Funktion wird deren **Hashwert** berechnet. Dabei sind nur die unveränderlichen Daten berücksichtigt. Sollte sich jedoch der Wohnort ändern, müsste ein neuer Ausweis erstellt werden. Alle Ergebnisse und Daten werden im Zahlensystem zur **Basis 62** gerechnet und ausgegeben [#1]. Basis 62 umfasst die folgenden Ziffern:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz  
(definiert vom Autor, nicht standardisiert)

Der Datenstring mit den eingebundenen persönlichen Daten des Antragstellers

***BergerKarlFriedrichWilhelm14.07.1952GroßkarolinenfeldSoltwedelBerlindeutsch***

führt zu folgendem Hashwert als Kennzeichen für die **Identität** des Antragstellers:

Hashwert (Basis 62): 21VtcLraTq  
hexadezimal: 615C8F186068F2  
dezimal: 27404842399983858

Der Hashwert (Basis 62) ist ein **eindeutiges Abbild** der persönlichen Daten des Antragstellers (**Identität**). Kollisionen sind ausgeschlossen. Infolge der unterschiedlichen persönlichen Daten der Antragsteller gibt es keinen doppelten Wert. Der Hashwert wird als **Zugangscod**e verwendet. Er steuert das gesamte Verfahren. Insoweit sind Seriennummern nicht erforderlich.

### **b) Passphoto des Antragstellers digitalisieren**

Zur weiteren Individualisierung wird das im Ausweis verwendete Passphoto des Antragstellers digitalisiert und der Hashwert des Bildes errechnet.



Angaben über den Ausweisinhaber

Bitte eingeben:  
Dateiname des digitalisierten Lichtbildes  
(\*\*\*\*bild.jpg)

Lichtbild (jpg): Meinfoto.jpg

Mit der CypherMatrix Funktion wird der Hashwert des Passbildes wie folgt ermittelt:

Hashwert (Basis 62): 4YUPj6sFACG  
hexadezimal: 3511EDF8E66ED908  
dezimal: 3.82409921188795828E+18



Für den Hashwert (Basis 62) generiert das Programm den zugehörigen **Strichcode**, der im unteren Bereich des Passbildes integriert wird. Mit einem Strichcodeleser kann die Übereinstimmung des Hashwertes (Basis 62) ohne weiteres mit dem von der

Ausstellungsbehörde gespeicherten Hashwert des Passbildes abgeglichen werden.

### c) Prüfung der Duplizität

Mit dem Zugangscode wird im REGISTER der Verwaltung geprüft, ob der Zugangscode schon registriert ist und somit der Antragsteller bereits einen elektronischen Personalausweis erhalten hat. Im positiven Fall verweigert das Programm die Weiterbearbeitung der Ausstellung und schaltet ab.

### d) Berechnung des Referenz

Grundlage für die Berechnung der **Referenz** ist ein Summenstring aus

#### **Identität + ConData + PhotoCode**

**ConData** ist ein internes Merkmal, das ausschließlich die Berechnung der Referenz unterstützt.

	Basis 62	hexadezimal	dezimal
Identität:	21VtcLraTq	615C8F186068F2	27404842399983858
ConData: +	1M8tw24WLB	414529B7C47021	1.83719189652726E+16
PhotoCode: +	4YUPj6sFACG	3511EDF8E66ED908	3.82409921188795828E+18

Summenstring: *21VtcLraTq1M8tw24WLB4YUPj6sFACG*

Der Summenstring wird der **CypherMatrix** Funktion unterworfen und für die resultierende „HashFunktionsReihe“ wird der Hashwert als **Referenz** errechnet.

Referenz = 3LP5dPu6ZG

Der **Referenzcode** wird an keiner Stelle des Programms sichtbar, er arbeitet im Verborgenen, vor allem als **Startsequenz** (Schlüssel) bei Verschlüsselungen der Datenströme zwischen den Bereichen: AUSSTELLUNG, ANWENDUNG und VERWALTUNG und als Ausgangspunkt für den **PINCode**.

### e) Bestimmung des PINCode

Der **PINCode** ist ein Steuerungsfaktor, der nur dem Ausweisinhaber bekannt sein sollte und für Maßnahmen verwendet wird, die allein vom Inhaber zu treffen sind. Grundlage für die Berechnung des PINCode ist die Referenz, die der Hashfunktion des **CypherMatrix** Verfahrens unterworfen wird. Der Hashwert des Ergebnisses ergibt dann den **PINCode**.

PINCode = fqhcoj1

Um die Zeichenfolge leichter behalten zu können, werden nur kleine Buchstaben und Ziffern verwendet (entspricht dem Zahlensystem zur Basis 36). Vordergründig dient der **PINCode** zur Freischaltung des Identitätsnachweises.

## f) Charakteristische Eigenschaften

Die drei aus den persönlichen Daten des Ausweisinhabers generierten Steuerungsparameter **Zugangscode**, **Referenz** und **PINCode** bilden in ihrer gegenseitigen Abhängigkeit eine datentechnische Einheit, die in ihrer Wirkung einer „**Signatur**“ der Identität des Ausweisinhabers gleich kommt. Vor allem, wenn bei jeder Prüfung die von der Verwaltung aktualisierten Daten fortgeschrieben werden.

Die Sensibilität des Verfahrens zeigt sich, wenn beispielsweise der Vorname mit **Kar**l**o** anstatt mit **Kar**l**** eingegeben wird bei ansonsten gleichen persönlichen Daten:

Zugangscode (Identität): 22NkdkGRzn  
Referenz: 3KX0odeUIS  
PINCode: unsikk1

Oder der Geburtstag weicht um einen Tag ab: **15.07.1952** anstatt **14.07.1952**

Zugangscode (Identität): 20MOitdkLR  
Referenz: 3JXPtF36iL  
PINCode: pbxjgjl

Wird im Passbild auch nur ein **Pixel** geändert, während alle Übrigen Daten gleich bleiben, ergeben sich für den Hashwert des Passbildes die folgenden Daten:

Hashwert (Basis 62): 4b0vyPVqAyW  
hexadezimal: 358B579B0606E280  
dezimal: 3.85827382910562368E+18

Bereichsgrenzen:

Das Zahlensystem zur Basis 62 hat 62 Ziffern. Zugangscode und Referenz umfassen 10 Stellen. Der PINCode mit 7 Stellen basiert auf 36 Ziffern.

Zugangscode (Identität):  $62^{10} = 8.392993659E+17$   
Referenz:  $62^{10} = 8.392993659E+17$   
PINCode:  $36^7 = 7.83641641E+10$

## g) Daten im Lesebereich des Ausweises

Der elektronische Personalausweis enthält einen Bereich für das automatische Auslesen bestimmter Daten, insbesondere für den Identitätsnachweis.

Der Zugangscode, ConData, PhotoCode und die persönlichen Daten 1,2,4,5,7,8,9,12, 13 und 14 werden im Lesebereich gespeichert. Die einzelnen Daten sind in einem Lesestring zusammengefasst, jeweils getrennt durch einen Backslash „\“:

Im Klartext:

21VtcLraTq\1M8tw24WLB\4YUPj6sFACG\D\IDD\Berger\Kar\14.07.1952\  
Großkarolinenfeld\Berlin\Lützowplatz 37\31.12.2020\ein\keine Vermerke

Die persönlichen Daten werden mit der **Referenz** verschlüsselt und zusammen mit den Steuerungsparametern im Lesebereich gespeichert:

21VtcLraTq\1M8tw24WLB\4YUPj6sFACG\w3uk5ToRVzzJ1AW5P2tMoilkrGncmnc  
gyqp7mL&r62JgDNCeQEh8#oFsPaiSa2XevHY1#ydroZ8Cl&jZB9ceB&surQtAa5jt  
aNmwbG3d6hYvPG9WGw1FmDax#1f&h7kyrrkzp7oe4MmbUrKREj1la5b6MKltBFxl

Bei einer Anforderung zum Auslesen der Daten werden die gespeicherten Sequenzen mit der **Referenz** wieder entschlüsselt und in ihre ursprüngliche Reihenfolge zurück verwandelt.

## h) Speicherung der Daten im BESTAND

Zur Verwaltung der ausgestellten Personalausweise erstellt das Programm zunächst eine Bestandsdatei als Grundlage für das Suchen und Finden der gespeicherten Daten eines Ausweisinhabers. Die Daten werden nicht verschlüsselt. Sie werden nur einmalig und kurzfristig übermittelt und stehen nur der Verwaltung zur Verfügung.

Dabei übernimmt der Zugangscode eine Suchfunktion für die in der Datenbank REGISTER gespeicherten und dem Ausweisinhaber zugeordneten Daten.

## i) Speicherung der Daten im REGISTER

Das REGISTER ist eine Datenbank im Bereich der Verwaltung. In ihr werden alle Daten, die im Zuge der Ausstellung eines Personalausweises anfallen, verschlüsselt gespeichert.

Zum Beispiel im vorliegenden Fall.

21VtcLraTq\3LP5dPu6ZG\1M8tw24WLB\QX#KQOW86YPxFGylyNgJE1SygUuR2FjC  
DYZeCTPmbMK93ha0WZz32QISFaPyg0hb5s66pAh3WGqKRDryzJcOBG27Ga6AyFDga  
WBGxk2kNutBDIhfwcTtGGrb1fU4HSJxrtoqvcfKWY63rfaLSNba74WrXjKglAalg  
i82Ban40kpiS6TGYLaUI&JmVeiuRZhfD5f8iiRxre0ZVX8DC&UARaObwPriS

Beim Aufruf zum Auslesen werden die Daten wieder entschlüsselt und ausgegeben.

## j) Aushändigung des Personalausweises

Nach Durchführung aller Eingaben entsteht der elektronische Personalausweis mit folgendem Bild



und kann dem Antragsteller ausgehändigt werden.

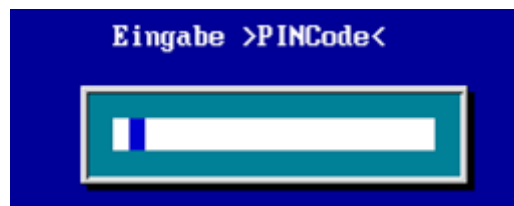
## B. Anwendungen

Für die möglichen Anwendungen des elektronischen Personalausweises sieht das Testprogramm folgende Bereiche vor:



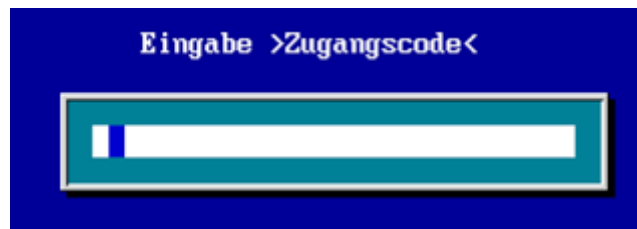
### a) Prüfung des Personalausweises

Zur Prüfung des elektronischen Personalausweises ist zunächst der **PINCode** einzugeben. Er muss vom Ausweisinhaber selbst eingegeben oder aber erfragt werden.



Ist der **PINCode** richtig, wird die Anfrage der Daten direkt an die REGISTER Datenbank der Verwaltung weitergegeben. Das begründet natürlich die Vermutung, dass der Besitzer auch der rechtmäßige Ausweisinhaber sei.

Ist der **PINCode** jedoch nicht bekannt oder wird er falsch eingegeben, erscheint eine entsprechende Fehlermeldung. In diesem Fall wird zusätzlich der **Zugangscod**e angefordert und weiter geschaltet.



Das kann mit Zeichen geschehen oder nur durch Drücken der [ENTER]-Taste. Die persönlichen Daten werden von der REGISTER Datenbank verschlüsselt geholt und mit der **Referenz** entschlüsselt. Wenn zwischenzeitlich im REGISTER einige Daten (Nr. 7, 8, 12, 13 oder 14) geändert worden sind, werden die Eintragungen im Lesebereich entsprechend fortgeschrieben. Dann erfolgt ein Abgleich der Daten (REG.Daten) mit den im Lesebereich (LES-Daten) gespeicherten Daten:

```

Ergebnis = 0
IF REG-Name = LES-Name THEN
  IF REG-Vorname = LES-Vorname THEN
    IF REG-Geburtstag = LES-Geburtstag THEN
      IF REG-Geburtsort = LES-Geburtsort THEN
        IF REG-Vermerke = „keine Vermerke“ THEN
          Ergebnis = 1
        END IF
      END IF
    END IF
  END IF
END IF
END IF

```

Mit dem Ergebnis = 1 wird die Übereinstimmung der Daten in der REGISTER Datenbank mit den im Lesebereich gespeicherten Daten bestätigt.

Auszug  
**Datenregister**

Ausweisinhaber: **Karl Berger**  
 noch Vornamen: **Friedrich Wilhelm**

Wohnort: **Berlin**  
 Adresse: **Lützowplatz 37**

Geburtsdaten: **14.07.1952 in Großkarolinenfeld**  
 gültig bis: **31.12.2020**  
 Sperrvermerke: **keine Vermerke**  
 Code Passphoto: **4YUPj6sFACG**

**Übereinstimmung wird bestätigt**

Um die Aktualität der gespeicherten Daten zu dokumentieren wird intern das Datum der Datenprüfung zusätzlich gespeichert. Besondere Beachtung kommt dem Feld **Sperrvermerke** zu, da hier abweichende Gültigkeitsmerkmale erscheinen könnten, wie: gesperrt, verloren oder ungültig.

## b) Identitätsnachweis

Vor der Einschaltung des Identitätsnachweises muss in laufender Sitzung noch die Prüfungsfunktion durchlaufen werden, anderenfalls erscheint eine entsprechende Aufforderung.

Im Falle einer externen Anfrage (Behörde oder Unternehmen) wird zunächst deren Identität und Berechtigung geprüft. Das Programm teilt den weiteren Ablauf, je nachdem ob der Internet-Partner eine Behörde ist oder ob es sich um ein Unternehmen

handelt. Im Fall einer Behörde geschieht das Auslesen des Lesebereichs automatisch. Bei einem Unternehmen muss der Ausweisinhaber durch die Eingabe seines **PINCodes** ausdrücklich seine Zustimmung erteilen.

Kontakt Adresse des Anfordernden

88/158/021/175  
Conrad Electronic

Weiter mit (ENTER)

Conrad Electronic  
berechtigt

Eingabe >Geheimcode PIN<

[Input field with a cursor]

Hat der Ausweisinhaber seine Zustimmung erteilt, werden folgende Daten als Nachweis der Identität des Inhabers an den Internet-Partner übermittelt.

Zur Identitätsfeststellung werden die folgenden  
in elektronischen Personalausweis gespeicherten  
Daten an den Anfordernden übermittelt:

Inhaber

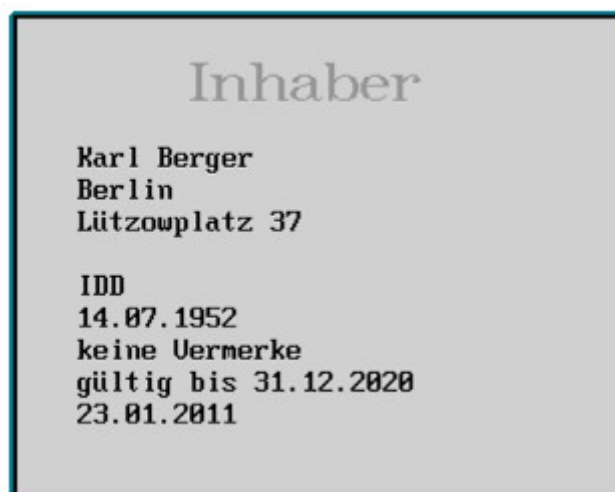
Karl Berger  
Berlin  
Lützowplatz 37

IDD  
Alter: 33-65  
keine Uermerke  
gültig bis 31.12.2020  
23.01.2011

Das Datum in der letzten Zeile gibt an, wann die letzte Abstimmung der persönlichen Daten mit den REGISTER-Eintragungen in der Verwaltung erfolgt ist. Insoweit wirken die Information wie eine aktuelle „Signatur“

Die Übermittlung der persönlichen Daten an die anfragende Behörde weicht in einem Punkt ab: es wird das genaue Geburtsdatum angegeben, während bei Informationen an ein Unternehmen nur die Altersgruppe mitgeteilt wird.

Die anfragende Behörde erhält folgende Daten als Nachweis der Identität des Ausweisinhabers:



### C. Verwaltung der Daten

Aufgabe der Verwaltung in den jeweils zuständigen Behörden ist die gesetzliche und sachgerechte Aufbereitung und Überwachung der Daten. Hierzu dienen insbesondere die Datenbanken für BESTAND und REGISTER mit allen in elektronischen Personalausweisen vergebenen Daten. Ordnungsmerkmal ist jeweils der **Zugangscode**, der zugleich ein Ausdruck für die **Identität** des Ausweisinhabers darstellt.

#### a) Datei BESTAND

In der Datei **BESTAND** werden die persönlichen Daten gespeichert, die zum Zugriff auf alle übrigen Daten eines Ausweisinhabers notwendig sind, wie:

**Name, Vorname, Wohnort und Zugangscode**

Eintragungen		
Nr:	Ausweis-Inhaber	Zugangs-Code
1	Mustermann geb. Berger, Erika Münch	2150ZyggeP
2	Dr. Lessing, Wolfgang Frankfurt	21FE08ttxz
3	<b>Berger, Karl Berlin</b>	<b>21UtcLraTq</b>
4	Möller, Cornelia Hamburg	22EGDSnSSD
5	Blankenburg, Werner Dresden	1LgsTMCq3U
6	Dr. Kellermann, Edgar Düsseldorf	20WCTffhFT
7	Jungblut, Hans-Oskar Stuttgart	1Lvg2dqjdo

Die Auswahl des zu suchenden Inhabers wird mit [TAB] und [UP] / [DOWN] gesteuert. Mit dem Zugangscode werden in der Datenbank REGISTER die zugehörigen weiteren Daten des Ausweisinhabers gefunden und ausgegeben.

## b) REGISTER und Änderungen

Die Datei enthält alle Daten, die bei der Ausstellung eines elektronischen Personalausweises eingegeben worden sind.

Ausweis-Register	
Familienname:	Berger
Rufname (Vorname):	Karl
weitere Vornamen:	Friedrich Wilhelm
Tag der Geburt:	14.07.1952
Ort der Geburt:	Großkarolinenfeld
Geburtsname der Mutter:	Soltwedel
Wohnort des Inhabers:	Berlin
Anschrift des Inhabers:	Lützowplatz 37
Doktorgrad:	
Staatsangehörigkeit:	deutsch
Ordens-, Künstlername:	
Gültigkeitsdauer:	gültig bis 31.12.2020
Identitätsnachweis:	ein
Sperrvermerke:	keine Vermerke
Code Passphoto:	4YUPj6sFACG

Die Daten stehen der Verwaltung zur Verfügung. Sie können jederzeit ausgelesen werden. Allerdings müssen sie auch ständig überwacht und anfallende Änderungen angepasst werden um die Aktualität des Verfahrens zu gewährleisten.

Als zu berücksichtigende Änderungen bietet das Programm die folgenden Korrekturmöglichkeiten:

1. Neuer Wohnort des Ausweisinhabers
2. Neue Anschrift des Ausweisinhabers
3. geänderte Gültigkeitsdauer
4. Änderung des Identitätsnachweises (ja/nein)
5. Sperrvermerke erteilt

The screenshot shows a software interface with a teal header bar containing the text "Änderung von Daten für den Ausweisinhaber". Below this is a grey bar with the label "Neuer Wohnort des Ausweisinhabers". Underneath is a white text input field with a blue cursor on the left. At the bottom of the screen is another grey bar with the text "Nur aktueller Wohnort".

Unter der Position **Sperrvermerke** können alle Einschränkungen in der Verwendung der Personalausweises eingetragen werden. Bei der nächsten Prüfung erhält sowohl der Ausweisinhaber als auch der Prüfer die Änderungen zur Kenntnis. Beim Identitätsnachweis führen Sperrvermerke entweder zum Blockieren der Anwendung oder sie werden in der Mitteilung an den Anfragenden sichtbar.

## D. Bemerkungen

### a) Datentechnik

Die Berechnung der Hashwerte wird mit der Hashwert-Funktion des CypherMatrix Verfahrens durchgeführt (final mode, Version: letzte Runde) [#2]. Die Hash-Sequenz beträgt 60 Bytes (bzw. alternativ 36 Bytes).

Verschlüsselungen werden ebenfalls mit der CypherMatrix Funktion vorgenommen [#3]. Das Verfahren verknüpft die Zeichen XOR und konvertiert dann die Zwischenwerte vom Bytesystem zur Basis 8 in das Bytesystem zur Basis 6. Das Verfahren ist nachweisbar (mathematisch) nicht zu brechen.

Im Fall einer Erweiterung des Verfahrens könnte mit einer **RFID** Funktion im engeren Umfeld des elektronischen Personalausweises der **Zugangscodes** – und nur der – ausgelesen werden. Wird der Zugangscodes an die REGISTER Datenbank weiter geleitet, ließen sich dort die persönlichen Daten des Ausweisinhabers kontrollieren und auswerten (z.B. zur Fahndung und Feststellung des jeweiligen Aufenthaltsortes des Ausweisbesitzers).

Das Programm ist in Power-Basic konzipiert. Zur Anpassung an aktuelle Programmiersprachen (C++, Unix) müsste die Software noch umgeschrieben werden.

### b) Vorteile

Für Verschlüsselungen ist kein allgemein gültiger Schlüssel notwendig, es werden nur individuelle und für den jeweiligen Ausweisinhaber unterschiedliche Schlüssel (**Referenz**) verwendet.

Der PINCode mit 7 Stellen im Zahlensystem zur Basis 36 ist wesentlich sicherer als ein PIN mit 6 Ziffern im dezimalen Zahlensystem.

Umfang der möglichen Varianten:

$$\begin{aligned} \text{PINCode: } & 36^7 = 7.83651641\text{E}+10 \\ \text{PIN: } & 10^6 = 1\,000\,000 \end{aligned}$$

Ein Umfang von 1 Million lässt sich mit heutigen Möglichkeiten leicht durch Iteration ausforschen.

Der Zugangscode als alleiniges Merkmal steuert die gesamte Verwaltung der allfälligen Daten. Seriennummern und Unterteilungen sind nicht erforderlich. Mit der aktuellen Abstimmung der Daten vor Inanspruchnahme des Identitätsnachweises wird außerdem die Wirkung einer aktuellen „Signatur“ erreicht.

Mit dem Zugangscode und seinen  $8.392993659\text{E}+17$  unterschiedlichen Sequenzen können alle Bürger in der Bundesrepublik Deutschland, ja sogar in ganz Europa, eindeutig identifiziert werden.

Das hier vorgestellte Verfahren kann ohne wesentliche Änderungen auch auf den elektronischen Reisepass angewendet werden.

### **c) Schwachstellen**

Als mögliche Schwachstelle zeigt sich die Situation in der ein gültiger und voll funktionsfähiger Ausweis gestohlen oder gefunden und vom Inhaber nicht sofort angezeigt wird. Eine dritte Person könnte dann den originalen Ausweis mit einem geänderten Passbild versehen, wobei der Strichcode aus dem alten Bild entfernt und auf das neue Bild übertragen wird.

Diesem Eingriff könnte nur dadurch begegnet werden, dass bei Vorlage und Prüfung des gefälschten Ausweises ein im REGISTER gespeichertes Passbild aktuell abgerufen und mit dem falschen Bild verglichen wird.

### **d) Sonstiges**

Um das Verfahren kennenzulernen, können Interessierte das zur Erläuterung der Zusammenhänge verwendete Programm beim Autor per e-mail

[eschnoor@multi-matrix.de](mailto:eschnoor@multi-matrix.de)

anfordern und einmal persönlich testen. Eine Weitergabe an Dritte setzt allerdings die ausdrückliche Zustimmung des Autors voraus. Der Autor ist außerdem bereit, sich jederzeit zu Diskussionen und persönlichen Erläuterungen von Zusammenhängen zur Verfügung zu stellen.

**München, im Januar 2011**

- [#1] Programm: NumberAD.exe (<http://www.telecypher.net/ZUSENDEN.HTM>)
- [#2] >CypherMatrix< als dynamische Hash-Funktion  
(<http://www.telecypher.net/DynahashD.pdf>)
- [#3] Verschlüsseln mit >CypherMatrix< (<http://www.telecypher.net/DynacodeD.pdf>)