

Der neue Personalausweis

... und was man damit tun könnte

10. Tagung DFN-Nutzergruppe Hochschulverwaltung

10. Mai 2011, Berlin

Marcus Pattloch (sicherheit@dfn.de)

- Der neue Personalausweis
 - Was ist das?
 - Was kann man damit Nützliches tun?
- Praktische Umsetzung am Beispiel DFN-PKI
- Ein paar kritische Gedanken
- Fazit

Der neue Personalausweis

Der neue Personalausweis

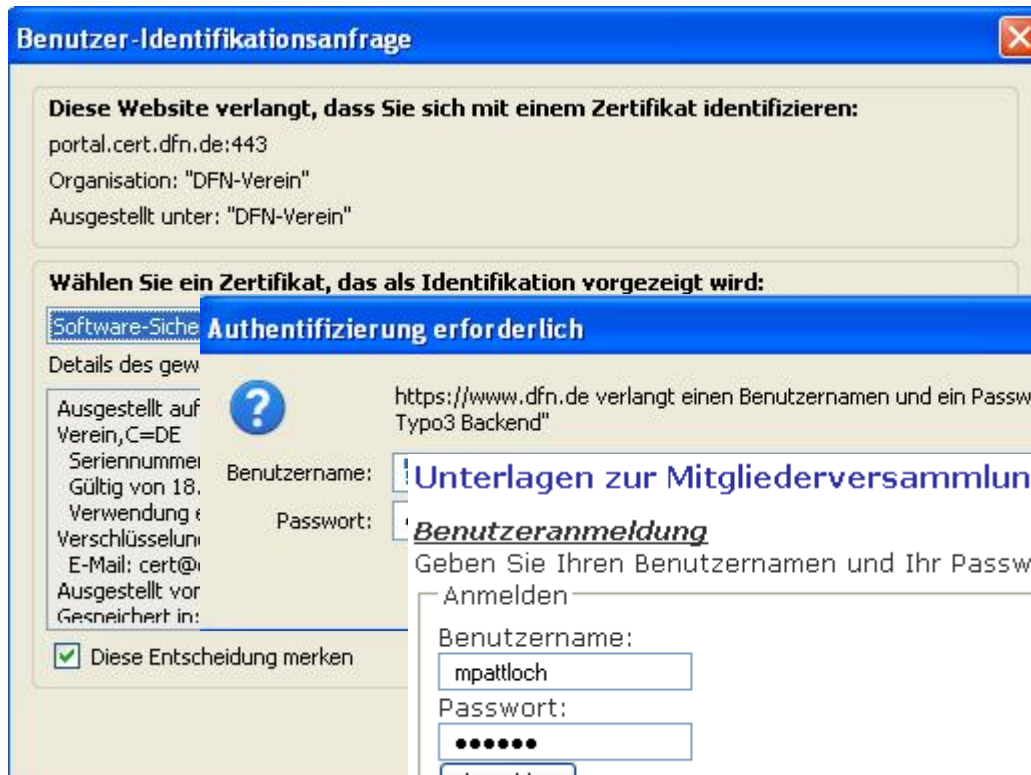
- Start des neuen Personalausweises (nPA) am 1. November 2010
- Nicht nur Sichtausweis, sondern auch als “elektronischer Ausweis im Internet” geplant



- eID-Funktion ist rechtlich geeignet, um
 - qualifizierte Zertifikate zu beantragen
 - Art. 4 “Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften” ergänzt die Signaturverordnung: “Die Identifizierung des Antragstellers kann auch mithilfe des elektronischen Identitätsnachweises gemäß § 18 des Personalausweisgesetzes erfolgen.”
- Folglich grundsätzlich geeignet, um eine Reihe von Diensten zur Identifizierung / Authentisierung zu unterstützen

- Frage: Gibt es Anwendungen im DFN, bei denen der nPA die Nutzer unterstützen kann?

DFN-CERT Portal



Benutzer-Identifikationsanfrage

Diese Website verlangt, dass Sie sich mit einem Zertifikat identifizieren:
portal.cert.dfn.de:443
Organisation: "DFN-Verein"
Ausgestellt unter: "DFN-Verein"

Wählen Sie ein Zertifikat, das als Identifikation vorgezeigt wird:

Software-Sicherheit: Authentifizierung erforderlich

Details des gewählten Zertifikats:

- Ausgestellt auf: Verein, C=DE
- Seriennummer: [unbekannt]
- Gültig von: 18. [unbekannt]
- Verwendung: [unbekannt]
- Verschüsselung: [unbekannt]
- E-Mail: cert@ [unbekannt]
- Ausgestellt vor: [unbekannt]
- Gesneuert in: [unbekannt]

Diese Entscheidung merken

Typo 3

DFN-MV

- Alles potentielle Anwendungsfälle für eID ...

- Frage: Gibt es Anwendungen im DFN, bei denen der nPA die Nutzer unterstützen kann?
- Antwort: Potentiell alle Fälle, bei denen sich Nutzer authentisieren müssen, z.B.
 - Zugriff auf das DFN-CERT Portal
 - Zugriff auf Typo3-Systeme
 - Zugriff auf geschützte Webbereiche, z.B. Vorstand oder Mitgliederversammlung
 - Bezug eines Zertifikats der DFN-PKI

Nutzung der eID am Beispiel der DFN-PKI

- Derzeit ca. 240.000 gültige Zertifikate
- Zertifikate in der DFN-PKI Global dürfen nur nach persönlicher Identifizierung des Zertifikatnehmers ausgestellt werden
 - bei zuständiger RA anhand eines amtlichen Ausweispapiers mit Lichtbild (CP 3.2.3 a)
 - per Postident (CP 3.2.3 b)
- Frage: Wie kann der elektronische Identitätsnachweis (eID) als weiteres Identifizierungsverfahren in der DFN-PKI unterstützt werden?

- Testphase des neuen Personalausweises
 - 1. Oktober 2009 - 31. Oktober 2010
 - Initiiert durch das BMI
 - Ziel: Finden von attraktiven Einsatzmöglichkeiten
- Teilnahme durch den DFN-Verein
 - Beschaffung von Testausweisen
 - Entwicklung einer exemplarischen Web-Anwendung am Beispiel DFN-PKI
 - Identifizierung in Test-Umgebung mit Testausweisen erfolgreich umgesetzt

Schritt 1 - Start Identifizierung



Schritt 1: Identifizierung

Legen Sie für die Ausstellung eines Zertifikats aus der DFN-PKI nun bitte Ihren neuen Personalausweis auf den Kartenleser und klicken Sie auf "Weiter".

Sie werden dann auf die Seite des vertrauenswürdigen eID-Providers [bremen online services](#) weitergeleitet, der die notwendigen Informationen aus Ihrem neuen Personalausweis ausliest und an den DFN-Verein übermittelt.

Weiter

Schritt 2 - Erkennen des nPA

Authentisierung mit dem Personalausweis.

Bitte haben Sie etwas Geduld während die Anwendung startet. Dieser Vorgang kann je nach Internetanbindung und Leistung des Computers wenige Minuten dauern.



Schritt 3 - Berechtigungszertifikat

Authentisierung mit dem Personalausweis.

Bitte haben Sie etwas Geduld während die Anwendung startet. Dieser Vorgang kann je nach Internetanbindung und Leistung des Computers wenige Minuten dauern.

AutentClient

1 Dienstanbieter

2 Daten auswählen

Der neue Personalausweis
Meine wichtigste Karte.

Dienstanbieter

Auf dieser Seite erhalten Sie Informationen über den Diensteanbieter, der die Daten aus Ihrem Personalausweis auslesen möchte. Außerdem erfahren Sie, wer die zuständige Stelle für die Einhaltung des Datenschutzes ist.

Anschrift:
Musterstraße 1
Berlin

E-Mail-Adresse:
info@ccepa.de

Verwendung der Daten:
Eintrittskarte

Zuständige Datenschutzaufsicht:
Muster Datenschutzbehörde

Die Berechtigung Daten aus Ihrem Personalausweis abzufragen, gilt vom 14.06.10 00:00 (lokale Zeit) bis 30.10.10 00:00 (lokale Zeit)

aa a ? ! 🔍 📄

➔ ❌

Schritt 4 - Freigabe Daten

Authentisierung mit dem Personalausweis.

Bitte haben Sie etwas Geduld während die Anwendung startet. Dieser Vorgang kann je nach Internetanbindung und Leistung des Computers wenige Minuten dauern.

AutentClient

1 Dienstanbieter

2 Daten auswählen

Der neue Personalausweis
Meine wichtigste Karte.

Daten auswählen

Auf dieser Seite können Sie die Datenfelder für die Übertragung an- oder abwählen. Bestimmen Sie dies über die Auswahlfelder.

Übertragen	Datenfeld	zustimmen	ablehnen
<input checked="" type="checkbox"/>	Vornamen	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Familiennamen	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Altersverifikation (über 18 Jahre)	<input checked="" type="radio"/>	<input type="radio"/>

Wählen Sie zum Übertragen der Daten die entsprechende Schaltfläche. Sie werden dann in einem neuen Fenster aufgefordert, Ihre persönliche Identifikationsnummer (PIN) einzugeben.

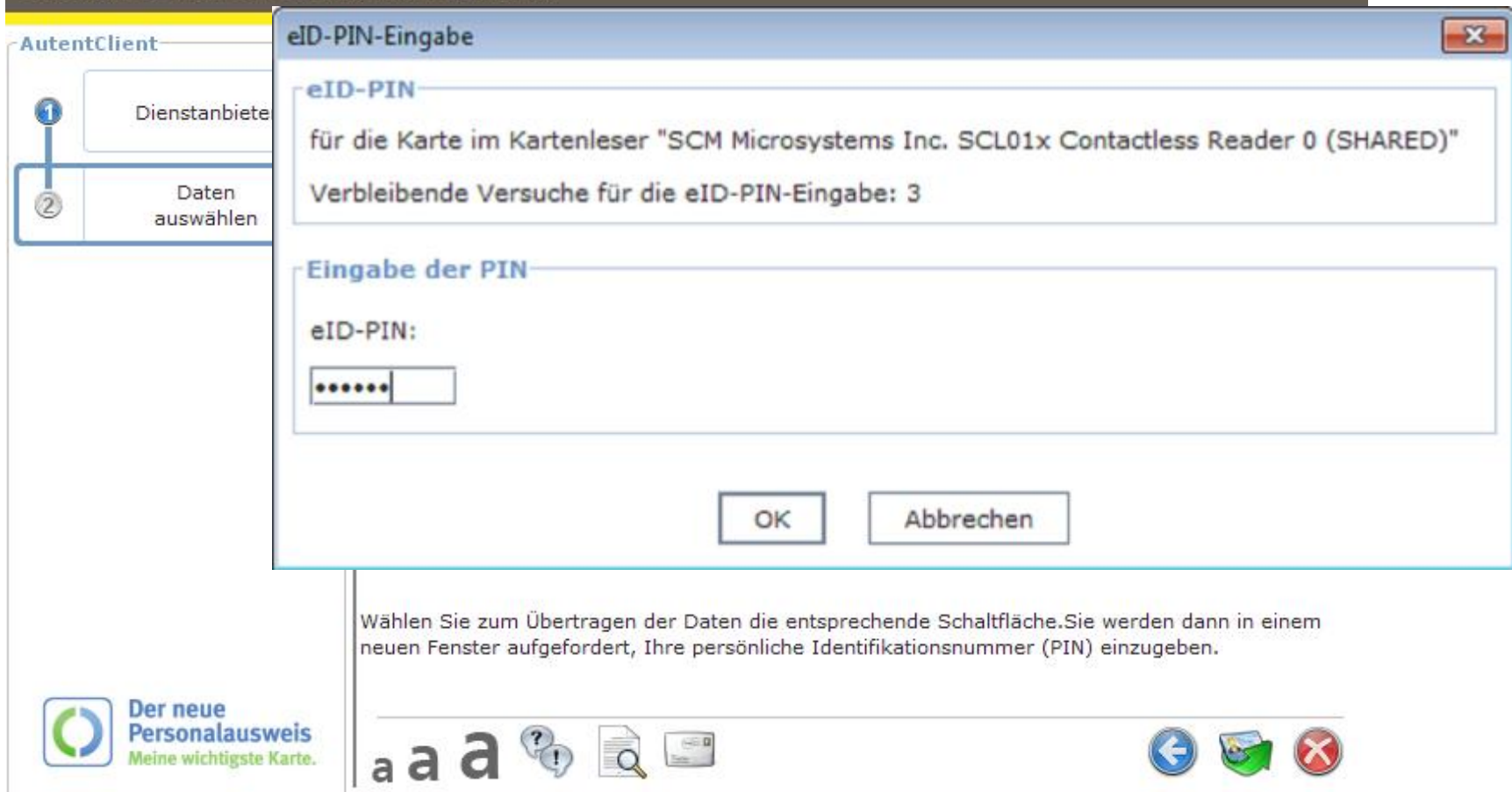
aa a ? ! [Magnifying Glass] [ID Card]

← ↻ ✖

Schritt 5 - Eingabe PIN

Authentisierung mit dem Personalausweis.

Bitte haben Sie etwas Geduld während die Anwendung startet. Dieser Vorgang kann je nach Internetanbindung und Leistung des Computers wenige Minuten dauern.



The screenshot shows a software interface for authenticating with a German ID card. On the left, a sidebar titled 'AutentClient' has two steps: '1. Dienstangebote' and '2. Daten auswählen', with the second step being active. The main window is a dialog box titled 'eID-PIN-Eingabe'. It contains the following text: 'eID-PIN für die Karte im Kartenleser "SCM Microsystems Inc. SCL01x Contactless Reader 0 (SHARED)"' and 'Verbleibende Versuche für die eID-PIN-Eingabe: 3'. Below this is a section titled 'Eingabe der PIN' with a label 'eID-PIN:' and a text input field containing six dots. At the bottom of the dialog are 'OK' and 'Abbrechen' buttons. Below the dialog, a text box reads: 'Wählen Sie zum Übertragen der Daten die entsprechende Schaltfläche. Sie werden dann in einem neuen Fenster aufgefordert, Ihre persönliche Identifikationsnummer (PIN) einzugeben.' At the bottom left is the logo for 'Der neue Personalausweis - Meine wichtigste Karte.' At the bottom right are several icons: three 'a' characters, a question mark, a magnifying glass, a document, a left arrow, a green folder, and a red 'X'.

Schritt 6- Zertifikatantrag



Schritt 2: Zertifikat beantragen

Es wurden über die Authentifizierung und Identifizierung die folgenden Daten ermittelt:

Vorname Name **HANS MUSTERMANN**
E-Mail **mustermann@uni-musterstadt.de**
Abteilung **RZ Uni Musterstadt**

Nach dem Akzeptieren der Zertifizierungsrichtlinie und einem Klick auf "Zertifikat beantragen" werden Sie in einem Dialog darüber informiert, dass diese Webseite einen Zertifizierungsvorgang einleiten will. Beantworten Sie diesen Dialog bitte mit "Ja".

- Ich stimme der [Zertifizierungsrichtlinie](#) zu.
- Ich stimme der [Veröffentlichung](#) des Zertifikats mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu.

Zertifikat beantragen

Schritt 7 - Zertifikatausstellung



Schritt 3: Warten auf Ausstellung

- ⌚ Es wird nun auf die Ausstellung des Zertifikats gewartet, was bis zu mehreren Minuten dauern kann. Nach der Ausstellung wird das Zertifikat automatisch installiert. Bitte beantworten Sie den dazu angezeigten Dialog mit "Ja".

Schritt 8 - Zertifikat erhalten



Das Zertifikat wurde installiert!

- ✓ Das ausgestellte Zertifikat befindet sich nun auf Ihrem Rechner. Bitte erstellen Sie eine Sicherheitskopie, indem Sie unter Internetoptionen -> Inhalte -> Zertifikate -> Eigene Zertifikate Ihr Zertifikat auswählen und dann "Exportieren..." klicken.

Weiter Informationen über den Umgang mit Ihrem Zertifikat erhalten Sie unter www.pki.dfn.de.

- eID ist eine interessante Ergänzung und funktioniert technisch, aber
 - Dienste umfassen mehr als Technik
- Sehr gewissenhafte Vorbereitung erforderlich
 - keine „technische Machbarkeitsstudie“ sondern Integration in einen sicherheitskritischen Dienst
 - Abstimmung Policy mit Dritten (Telekom, Mozilla)
 - Erfüllung Kriterien Audits (z.B. Dokumentationspflichten)
 - Berücksichtigung datenschutzrechtlicher Anforderungen
 - Verzahnung mit Prozessen bei DFN-Anwendern
 - betriebliche Prozesse innerhalb der DFN-PKI

Ein paar kritische Gedanken

- Regierungsbegründung zum PAuswG (BT-Drs. 16/10489, S. 40 zu § 14):
 - „dass die **Erhebung** und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig **nur über** die dafür vorgesehenen Wege erfolgen darf. Dies sind für nichtöffentliche und öffentliche Stellen der **elektronische Identitätsnachweis** und für zur hoheitlichen Identitätsfeststellung berechnigte Behörden der Abruf der elektronisch gespeicherten Daten einschließlich der biometrischen Daten. **Weitere Verfahren z. B. über die optoelektronische Erfassung** („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich **sollen ausdrücklich ausgeschlossen werden.**“

- In einer ergänzenden Stellungnahme des BMI zur Vervielfältigung von Ausweisdokumenten wird dies noch genauer erläutert:
 - *"[...] Diese Klarstellung war u. a. deshalb erforderlich, weil im Falle einer künftigen Vervielfältigung des neuen Personalausweises zusätzliche Sicherheitsprobleme entstünden. Denn auf dem neuen Personalausweis ist die Berechtigungs-Nummer abgedruckt. Diese soll grundsätzlich nur dem Ausweisinhaber bekannt sein, könnte durch Kopieren des Ausweises aber in Umlauf geraten."*
- Das Anfertigen einer Fotokopie des neuen Personalausweises soll demnach ausdrücklich nicht von § 14 PAuswG gedeckt sein.

- § 1 Abs. 1 PAuswG
 - „... *Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Dies gilt nicht für zur Identitätsfeststellung berechnigte Behörden sowie in den Fällen der Einziehung und Sicherstellung..*“
- Heise Online (9.11.2010 16:51)
 - *“Hotels, Fitnessstudios oder ganz allgemein Unternehmen, die von Besuchern beim Zutritt des Werksgeländes den Personalausweis kassieren, müssen umdenken und auf andere Verfahren umsatteln.”*

- Vom Bürger zu wählende PIN ist 6-stellig
 - aufgedruckte Berechtigungs-Nummer (CAN) ist 6-stellig
 - aufgedrucktes Geburtsdatum ist 6-stellig
- Hinweis auf “https://www.ausweisapp.bund.de/pweb/filedownload/download_pre.do”:
 - “Bitte wählen Sie dafür keine leicht zu erratende Nummer wie z.B. ein Geburtsdatum oder 123456.”
- Warum wird das nicht technisch verhindert?

- 9. November 2010
 - Sicherheitslücke in der Version 1.0.1 aufgrund zweier Fehler in der Auto-Update-Funktion
 - Update im Januar 2011
- Weitere Schlagzeilen bei Heise online:
 - Schlanke AusweisApp soll Personalausweis Schwung verleihen (22.2.2011)
 - Neuer Personalausweis: Firefox 4 deaktiviert AusweisApp-Erweiterung (24.3.2011)
- Probleme Verfügbarkeit AusweisApp für Mac / Linux

- Kein automatischer Roll-out von qualifizierten Zertifikaten für “Alle”
 - Neuer Personalausweis wäre technisch dafür vorbereitet
- Kartenleser
 - Klasse 1: Ohne Pinpad und Display
 - nicht empfehlenswert
 - wurde aber massiv verbreitet
 - Klasse 2: Mit Pinpad ohne Display
 - Klasse 3: Mit Pinpad und mit Display

Fazit

- Der nPA ist vom technischen und organisatorischen Aufbau grundsätzlich eine gute Sache!
 - Neue Anwendungen werden durch die eID möglich
 - (Noch) gibt es einige Kritikpunkte, die die Nutzung in der Praxis verkomplizieren
- Mehrere potentielle Nutzungsszenarien im DFN-Umfeld erkennbar, dabei
 - gewissenhafte Vorbereitung erforderlich in Bezug auf Anpassung der Policies, Betriebsprozesse, organisatorische Abläufe und Technik