Der neue Personalausweis

... und was man damit tun könnte

10. Tagung DFN-Nutzergruppe Hochschulverwaltung

10. Mai 2011, Berlin

Marcus Pattloch (sicherheit@dfn.de)

Übersicht

- 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

Neuer Personalausweis

- 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

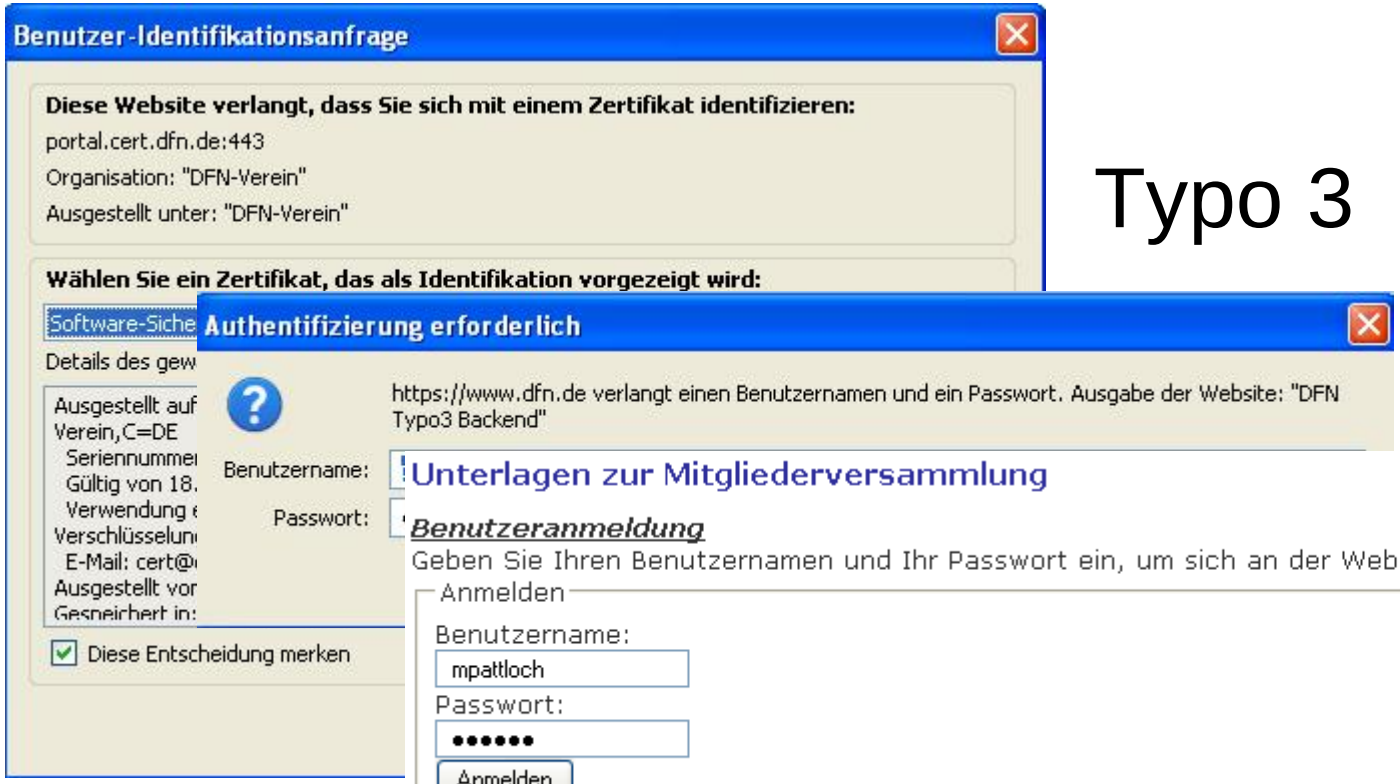
Mögliche Nutzung im DFN-Umfeld

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

Heutige Nutzer-Authentifizierung

DFN Deutsches Forschungsnetz

DFN-CERT Portal



Typo 3

DFN-MV

- Alles potentielle Anwendungsfälle für eID ...

Mögliche Nutzung im DFN-Umfeld

- 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

Beispiel: DFN-PKI

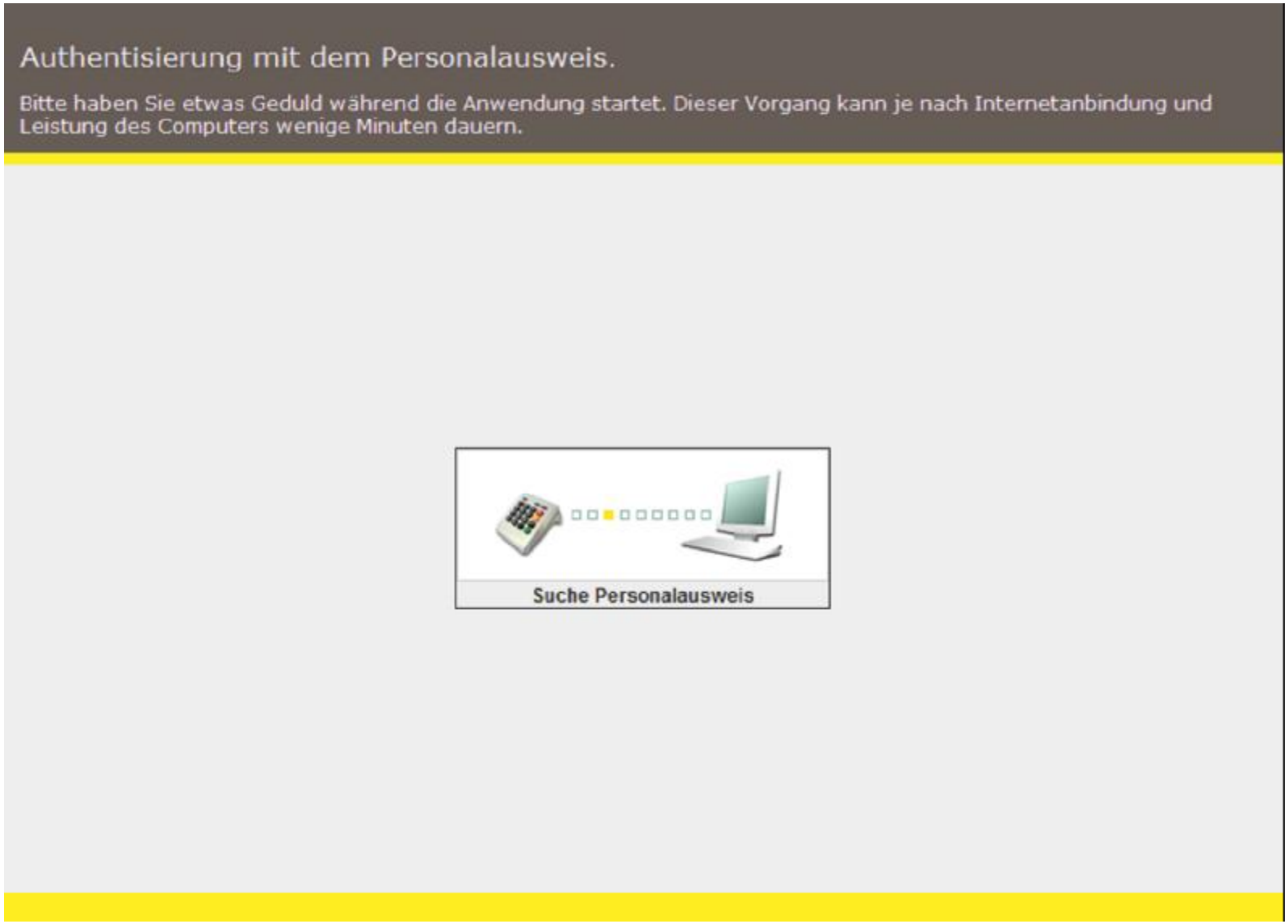
- Derzeit ca. 240.000 gültige Zertifikate
- Zertifikate in der DFN-PKI Global dürfen nur nach persönlicher Identifizierung des Zertifikatnehmers ausgestellt werden
  - bei zuständiger RA anhand eines amtlichen Ausweispapiers mit Lichtbild (CP 3.2.3 a)
  - per Postident (CP 3.2.3 b)
- Frage: Wie kann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

Der offene Anwendungstest

- 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

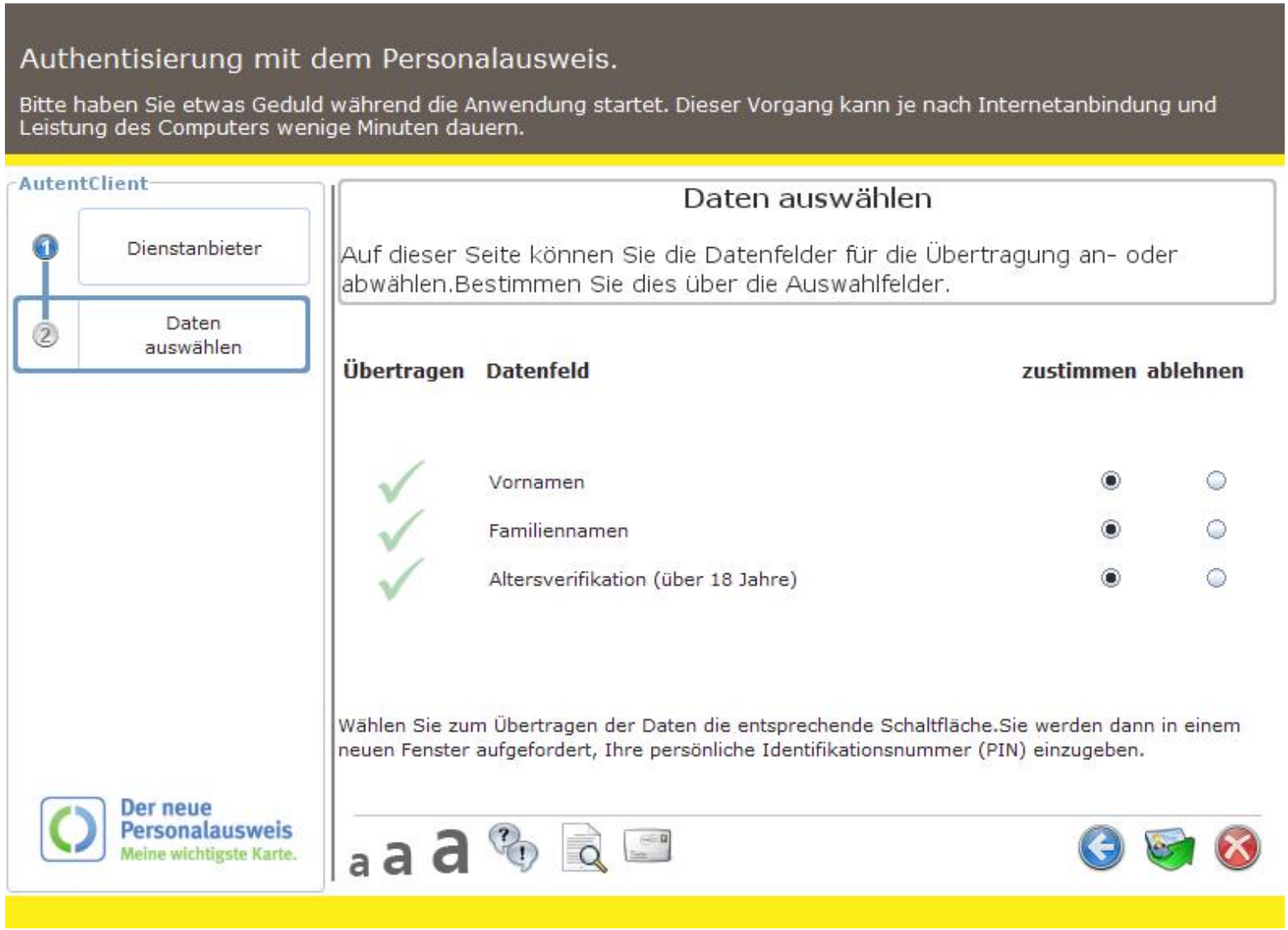
Schritt 1 - Start Identifizierung

Schritt 2 - Erkennen des nPA

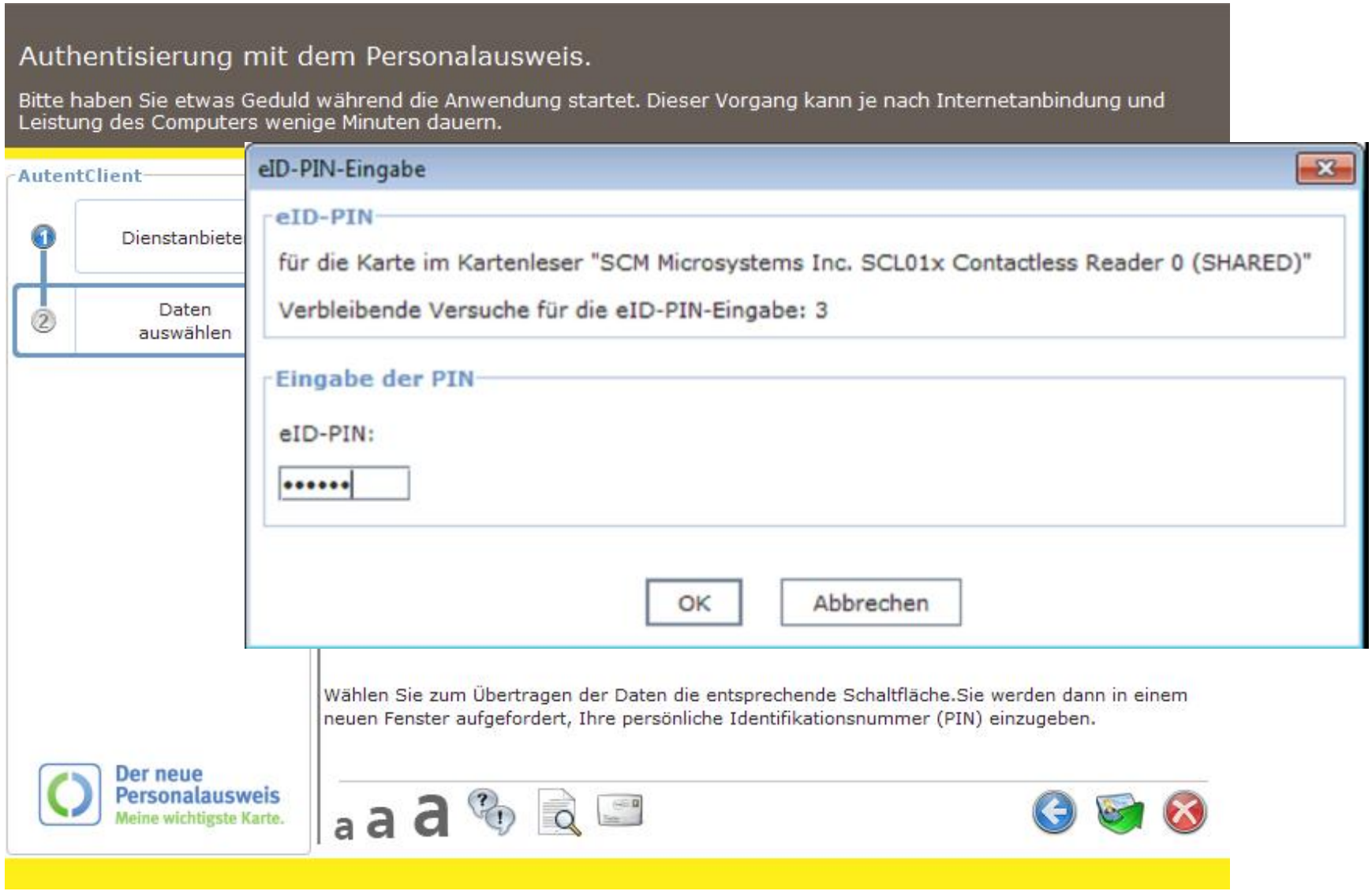


Schritt 3 - Berechtigunszertifikat

Schritt 4 - Freigabe Daten



Schritt 5 - Eingabe PIN



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".

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

Zertifikat beantragen

Schritt 7 - Zertifikatausstellung

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.

Nutzung nPA in der DFN-PKI

- 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

„Kopierverbot“ (1)

- 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 berechtigte 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.“*

„Kopierverbot“ (2)

- 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 Personal-ausweises soll demnach ausdrücklich nicht von § 14 PAuswG gedeckt sein.

„Hinterlegungsverbot“

- § 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 berechtigte 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.”*

PIN

- 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?

AusweisApp (Bürgerclient)

- 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

Weitere Punkte

- 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

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