Der neue Personalausweis

IHK Offenbach, 18.11.2010

Oliver Berndt
B&L Management Consulting GmbH

B&L Management Consulting GmbH

B&L Management Consulting GmbH

Unser Leistungsspektrum

- **Dokumenten-Management**
- **Elektronische Signaturen**
- **E-Mail Management**
- **Wissens-Management**

- **Analysen**
- **Konzepte**
- **Anbieterauswahl**
- **Projektmanagement**
- **Systemeinführung**
- **Outsourcing**
- **Coaching**
- **Migration**

B&L, Lösungen für Ihren unternehmerischen Erfolg.

B&L Management Consulting GmbH

Agenda

- Generelles zum nPA
- Was ist neu am „neuen Personalausweis“?
- Anwendungsbeispiele
- eID-Funktion
- Elektronische Signatur mit dem nPA
- Sicherheit und Angriffe
- Haftung für ID-Mißbrauch

B&L Management Consulting GmbH

Generelles zum nPA

Hoheitliche Funktionen, wie bisher

- Pflicht für alle Deutschen ab Alter von 16 Jahre
- Wahlfrei: 2 Fingerabdrücke speicherbar
- Lesbar nur für Polizei, Zoll, Meldebehörden
- Gültigkeit (> 24 Jahre): 10 Jahre
- Kosten(> 24 Jahre): 28,80 €

Quelle: BMI, Alles Wissenswerte zum neuen Personalausweis, August 2010

Was ist neu am „neuen Personalausweis“?

Kontaktlose Lesemöglichkeit der Daten

- Zusätzliche Funktionen durch Chip
  - Electronic Identity, eID
  - Qualifizierte Signatur
- Durch die Eingabe Ihrer PIN können Sie max. freigeben:
  - Vor- und Familienname, ggf. Ordens- und Künstlername oder Doktorgrad
  - „D“ für Bundesrepublik Deutschland
  - Angaben zur Über- oder Unterschreitung eines bestimmten Alters (Altersbestätigung)
  - Geburtstag und Geburtsort
  - Anschrift
  - Dokumententyp
  - Angabe, ob der eigene Wohnort einem abgefragten Wohnort entspricht (Wohnortbestätigung)
  - Pseudonyme Kennung (Dienste-/Kartenspez. Kennzeichen)

B&L Management Consulting GmbH

Was ist eID-Funktion?

Identifizierung gegenüber Diensteanbietern im Internet

- Berechtigungszertifikat für Daten des PA
  - Diensteanbieter muss bei BVA Antrag für Daten stellen „Erforderlichkeit" detailliert darlegen
    - Ggf. nur Altersverifikation (z.B. Ü18 Ja/Nein) oder Wohnortverifikation (z.B. regionale Angebote)
  - Zum 1.11.2010 liegen ca. 150 Anträge vor
- Sicherheit
  - eID abschaltbar
  - Nutzung erst ab 16 Jahre möglich
  - Schutz über 6-stellige PIN-Eingabe
  - Nur ausgewählte Daten werden weitergeleitet
  - Sämtliche Datenübertragungen erfolgen verschlüsselt
  - Chip ist „Sicherheitsanker"
    - Geheimer Schlüssel nicht auslesbar

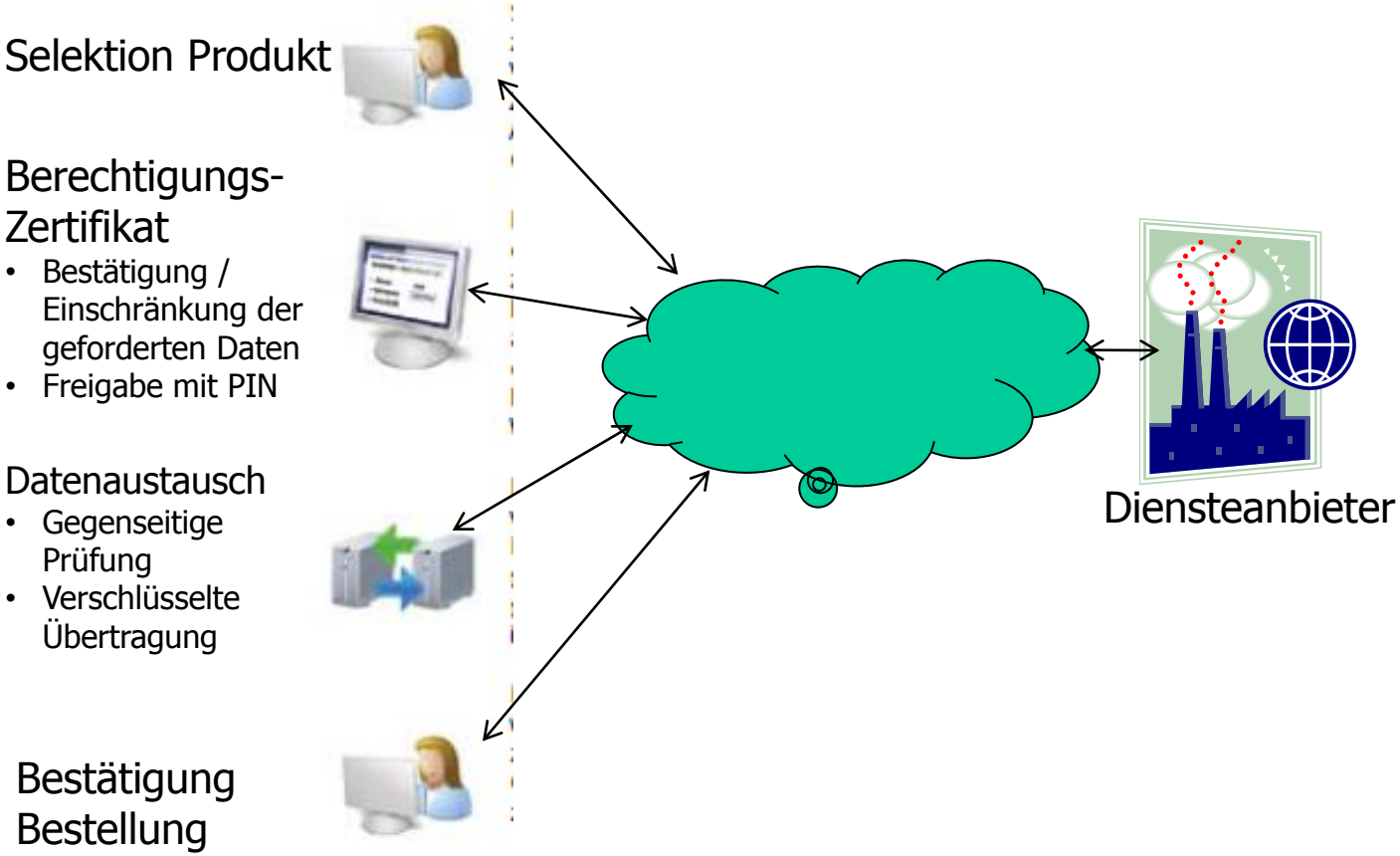
B&L Management Consulting GmbH

Quelle: BVA, Vortrag K. Wolter, CAST-Forum, 28. Oktober 2010

Verfahren der eID im Web

Quelle: dpa, hier aus Rheinzeitung

Beispiel Online-Einkauf



Quelle: BMI, Alles Wissenswerte zum neuen Personalausweis, August 2010

Weitere Anwendungsbeispiele

Online-Registrierung

Automaten, z.B.
- Fahrkarten
- Zigaretten

Zugang mit Pseudonym

Qualifizierte Signatur

Altersbestätigung

Autom. Füllen Formulare

Behördengänge

Barrierefreie Angebote

Zutrittskontrolle

B&L Management Consulting GmbH

Quelle: BMI, Alles Wissenswerte zum neuen Personalausweis, August 2010

Diensteanbieter am 5.11.2010

- Banken
  - Deutsche Kreditbank
  - Sparkasse Jena-Saale
  - Teambank AG (easycredit)
- Behörden
  - Anstalt für kommunale DV in Bayern, AKDB
  - Bay. Landesamt für Steuern
  - Deutsche Rentenversicherung
  - Innenministerium Baden- Württ.
  - Stadt Hagen
  - Stadt Münster
- Sonstige
  - Bremen online services GmbH
  - Deutsche Emissionshandels-stelle
  - Fujitsu Tech. Solutions GmbH
  - Tönjes Holding AG
  - VZnet Netzwerke Ltd.
- Versicherungen
  - Allianz Deutschland AG
  - Cosmos Lebensversicherungs AG
  - Easy Login GmbH (DL)
  - Gesamtverband Deutsche Versicherungswirtschaft e.G.
  - Gothaer Allg. Versicherung AG
  - Hannoversche LV AG
  - HUK24 AG
  - LVM, Landwirtschaftlicher Versicherungsverein
  - Provinzial Rheinland LV AG
  - S-direkt Versicherung AG
  - Versicherungswirtschaftlicher Datendienst GmbH (DL)
  - Zürich Vertriebs GmbH

B&L Management Consulting GmbH

Quelle: Web-Seite der Bundesnetzagentur

Nutzen eID

- Zeitersparnis durch Online-Transaktionen 24x7, z.B.
  - Kein Post-Ident-Verfahren erforderlich
  - Weniger Behördengänge
- Sicherheit für beide Seiten im (anonymen) Online-Handel
- Berechtigungszertifikat
  - Name, Adresse, E-Mail des Diensteanbieters
  - Zweck der Datenübermittlung
  - Zuständige Datenschutzaufsichtsbehörde
  - Gültigkeit des Berechtigungszertifikats
- Identitätsschutz, z.B.
  - gegen Phishing beim eBanking
  - in sozialen Netzwerken

B&L Management Consulting GmbH

HW/SW-Voraussetzung für Nutzung

- PC mit
  - Windows, MacOS, Linux
  - Internet Explorer, Firefox, Safari
  - Ab 3.2011: Outlook, Thunderbird, Apple Mail, kmail
- Software
  - „AusweisApp": Anwendung für die Nutzung der Zusatzfunktionen im Internet
  - Bei BMI herunterzuladen (www.ausweisapp.bund.de)
- Hardware:
  - 3 Kategorien (gemäß BSI TR 03119) von Kartenlesern
    - Basisleser (Cat B)
    - Standardleser (Cat S)
    - Komfortleser (Cat K)
  - Nur zertifizierte Geräte erlaubt

B&L Management Consulting GmbH

Quelle: BSI, Vortrag J. Bender, CAST-Forum, 28. Oktober 2010

Organisatorische Voraussetzung für Nutzung neuer Funktionen

„Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Personalausweisinhaber übermittelt und dieser in der Folge seine Geheimnummer eingibt."

- Beschaffung IT-Sicherheitskit oder
  - Beschaffung Hardware
  - Download und Installation der AusweisApp auf eigenem PC
- PIN
  - Nach Beantragung Lieferung
    - Transport-PIN (5-Stellen), PUK, Sperrkennwort
  - Einrichtung eigener 6-stelliger PIN
- Bei Verlust:
  - Sperren lassen über Hotline 0180-1-33 33 33
- Hinterlegung des PA, z.B. im Hotel, nicht mehr erlaubt

B&L Management Consulting GmbH

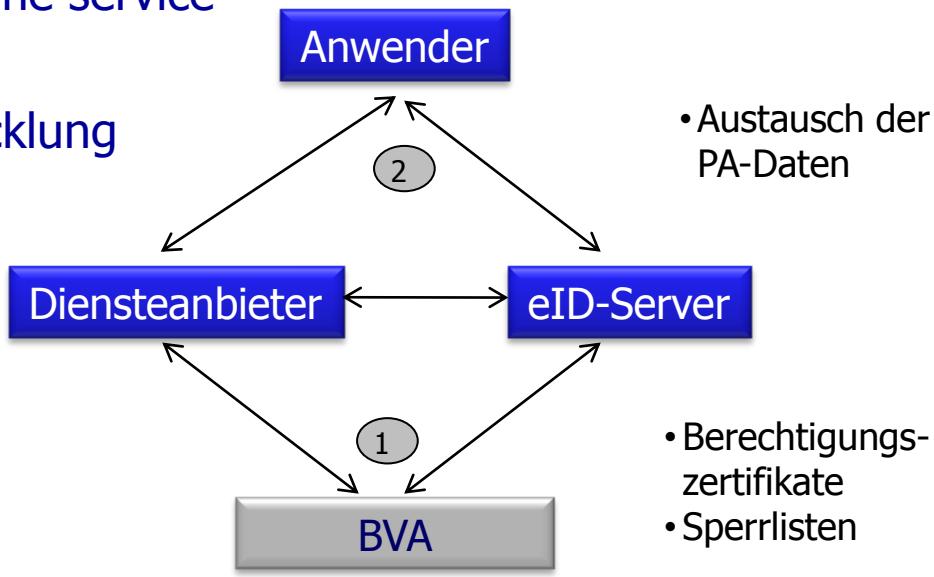
eID-Server

Diensteanbieter benötigt eID-Server

- Gegenüber zum AusweisApp
- eID-Server kann über Dienstleister genutzt werden
- Erforderlich um Berechtigungszertifikat zu prüfen

Software-Anbieter

- Bremen online service
- OpenLimit
- Eigenentwicklung möglich



- Austausch der PA-Daten
- Berechtigungs-zertifikate
- Sperrlisten

B&L Management Consulting GmbH

Signatur mit nPA

Qualifiziert Signieren soll ab März 2011 möglich sein

- nPA kann SmartCard für qualifizierte Signaturen ersetzen
  - Enthält aber kein Zertifikat
  - Zertifikate müssen – wie heute - bei den Trust Centern gekauft, geladen und aktiviert werden
  - Benötigt eigene PIN
- Nur mit Komfort-Leser (Tastatur und Display) zugelassen
  - Am 1.11.2010 keine zertifizierten Leser verfügbar
- Qualifizierte Signatur ist natürlicher Unterschrift rechtlich gleich gestellt

B&L Management Consulting GmbH

Vergleich eID und Signatur

Verträge ohne Formerfordernis können über eID geschlossen werden

eID
- „Das bin ich"
- Anzeige Identität des Diensteanbieters
- Anzeige der angefragten Daten
- Personendaten-Freigabe mit PIN
- Personendaten-Übertragung
- Beispiele: Anmeldung/Registrierung, Altersnachweis, Pseudonym

Qualifizierte Signatur
- „Das habe ich unterschrieben"
- Anzeige des zu unterschreibenden Dokuments oder der E-Mail
- Signieren mit PIN-Eingabe
- Prüfung der Signatur durch Empfänger
- Beispiele: Unterschreiben von Verträgen, Vollmachten, E-Mails

B&L Management Consulting GmbH

Quelle: BVA, Vortrag K. Wolter, CAST-Forum, 28. Oktober 2010

Infrastruktur

Im Hintergrund ist umfangreiche Organisation und Technik erforderlich

- Geregelt in TR 03127 des BSI
- Bundesamt für die Sicherheit in der Informationstechnik (BSI)
  - Betreiber der Root-CA/Trust-Center
- Bundesverwaltungsamt
  - Vergabestelle für Berechtigungszertifikate (VfB) als Betreiber der Registration Authority (RA)
  - Sperranforderung mit Sperrhash
  - Dienste-/kartenspezifische Sperrlisten
- Zertifikateanbieter
  - Ausstellung der Berechtigungszertifikate

B&L Management Consulting GmbH

Antragstellung Berechtigungszertifikat

- „Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht,
  - seine Identität dem Personalausweisinhaber nachzuweisen und
  - die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis anzufragen (§ 2 Abs. 4 PAuswG).“

Antragstellung bei Vergabestelle im Bundesverwaltungsamt

Vergabestelle der Berechtigung

Beschaffung bei (privaten) Zertifikateanbietern

B&L Management Consulting GmbH

Quelle: Leitlinie für die Vergabe von Berechtigungen für Diensteanbieter nach § 21 Abs. 2 Personalausweisgesetz

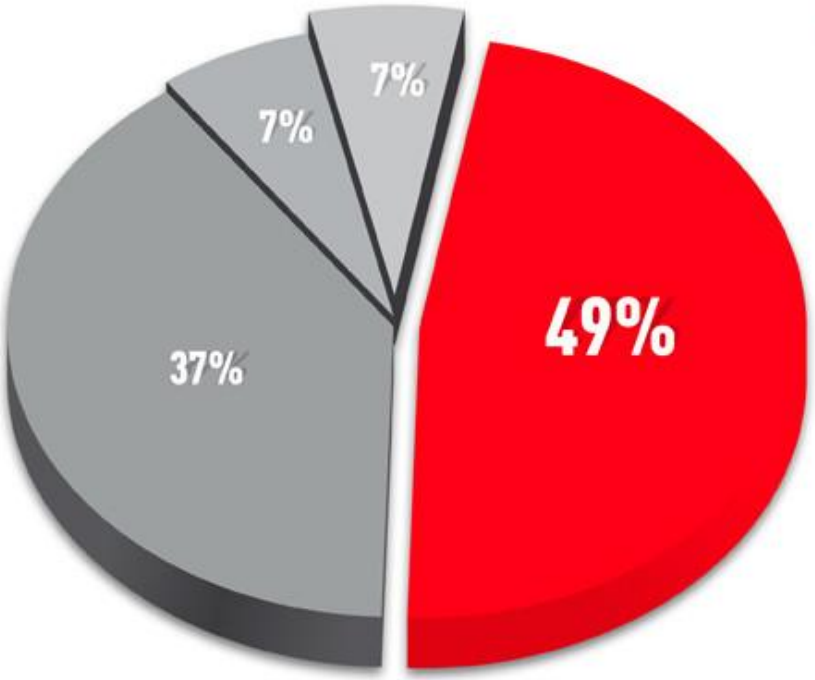
Voraussetzungen für Berechtigung

Ziel ist Datensparsamkeit

- Voraussetzungen des § 21 PAuswG erfüllen:
  - Nachweis über die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Geschäftszweck
  - Maßnahmen zu Datenschutz und –sicherheit
  - der angegebene Geschäftszweck ist nicht rechtswidrig
  - der Geschäftszweck besteht nicht in der geschäftsmäßigen Übermittlung der Daten und es liegen keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vor
  - keine Anhaltspunkte für missbräuchliche Verwendung der Berechtigung zur Nutzung der eID-Funktion
- Berechtigungen sind zeitlich begrenzt

B&L Management Consulting GmbH

Ist die Skepsis gerechtfertigt?



49 %	Ich stehe dem Ganzen skeptisch gegenüber und werde den neuen Ausweis vorerst nicht beantragen
37 %	Es ist nur eine Frage der Zeit, bis Cyberkriminelle den nPA knacken und deshalb werde ich meinen Ausweis nicht online nutzen
7 %	Ich habe volles Vertrauen in das staatliche Sicherheits-konzept des nPA und werde ihn auch im Internet verwenden
7 %	Ich höre jetzt zum ersten Mal von diesem neuen Ausweis

Quelle: Avira-Umfrage, Computerbild, 20.10.2010

Bisherige Angriffe

Neue Funktionen lassen sich deaktivieren

- Angriff durch PIN-Abgriff
  - Basisleser erfordert PIN-Eingabe über Tastatur
  - Virus / Trojaner (keylogger) könnte PIN-Eingabe mitlesen
  - Wenn Angreifer in Besitz der Karte kommt, z.B. auf Leser liegen gelassen, ist Missbrauch möglich
  - ABER:
    - Wer Viren hat, hat ein generelles Problem
    - Vorsorge ohnehin notwendig
  - BSI-Empfehlung
    - Virenschutz und Firewall
    - Zertifizierte Komponenten
- Deaktivierung des Chips
  - Zusatzfunktionen nicht mehr verfügbar
  - Keine sensiblen Daten lesbar
  - Hoheitliche Funktion nicht beeinträchtigt, weil unabhängig

B&L Management Consulting GmbH

Haftung für Identitätsmissbrauch und neuer Personalausweis 1/2

Der Ausweisinhaber kann bei Schäden aufgrund von Fehlfunktionen z.T. andere in die Haftung nehmen

1. Das Risiko des Fehlschlagens der eID trägt der Ausweisinhaber
   a. Andere können haften, wenn sie zum Fehlschlagen beigetragen haben
2. Erhebliche Haftungsrisiken trägt Diensteanbieter (Authentisierungsnehmer)
   a. Gilt auch für öffentliche Verwaltung
3. Hersteller und Lieferanten der Komponenten haften gegenüber ihren Abnehmern
   a. Bei kostenloser Abgabe, nur Haftung für grobes Verschulden

B&L Management Consulting GmbH

Quelle: Vortrag Prof. Dr. G. Borges, CAST-Forum, 28. Oktober 2010

Haftung für Identitätsmissbrauch und neuer Personalausweis 2/2

Der Diensteanbieter trägt primäres Ausfallrisiko

1. Das Risiko des Missbrauchs der eID trägt der Getäuschte (Diensteanbieter)
   a. Ausweisinhaber haftet in Vertragsverhältnissen , wenn er seine Sorgfaltspflicht verletzt
2. Diensteanbieter (Authentisierungsnehmer) haftet, wenn er unsichere Authentisierungssysteme verwendet oder
   a. Zumutbare Maßnahmen zur Echtheitsprüfung unterlässt.

B&L Management Consulting GmbH

Quelle: Vortrag Prof. Dr. G. Borges, CAST-Forum, 28. Oktober 2010

Fragen?

Dann sprechen Sie uns einfach an.

Kontakt: Dipl. Wirtsch.-Ing. Oliver Berndt

B&L Management Consulting GmbH
Frankfurt / Rosenheim
Tel.: 069-133093-0
E-Mail: berndt@bul-consulting.de
Internet: www.bul-consulting.de

B&L, Architekten für ECM und DMS.

B&L Management Consulting GmbH