Selbstbestimmtes Handeln im Netz

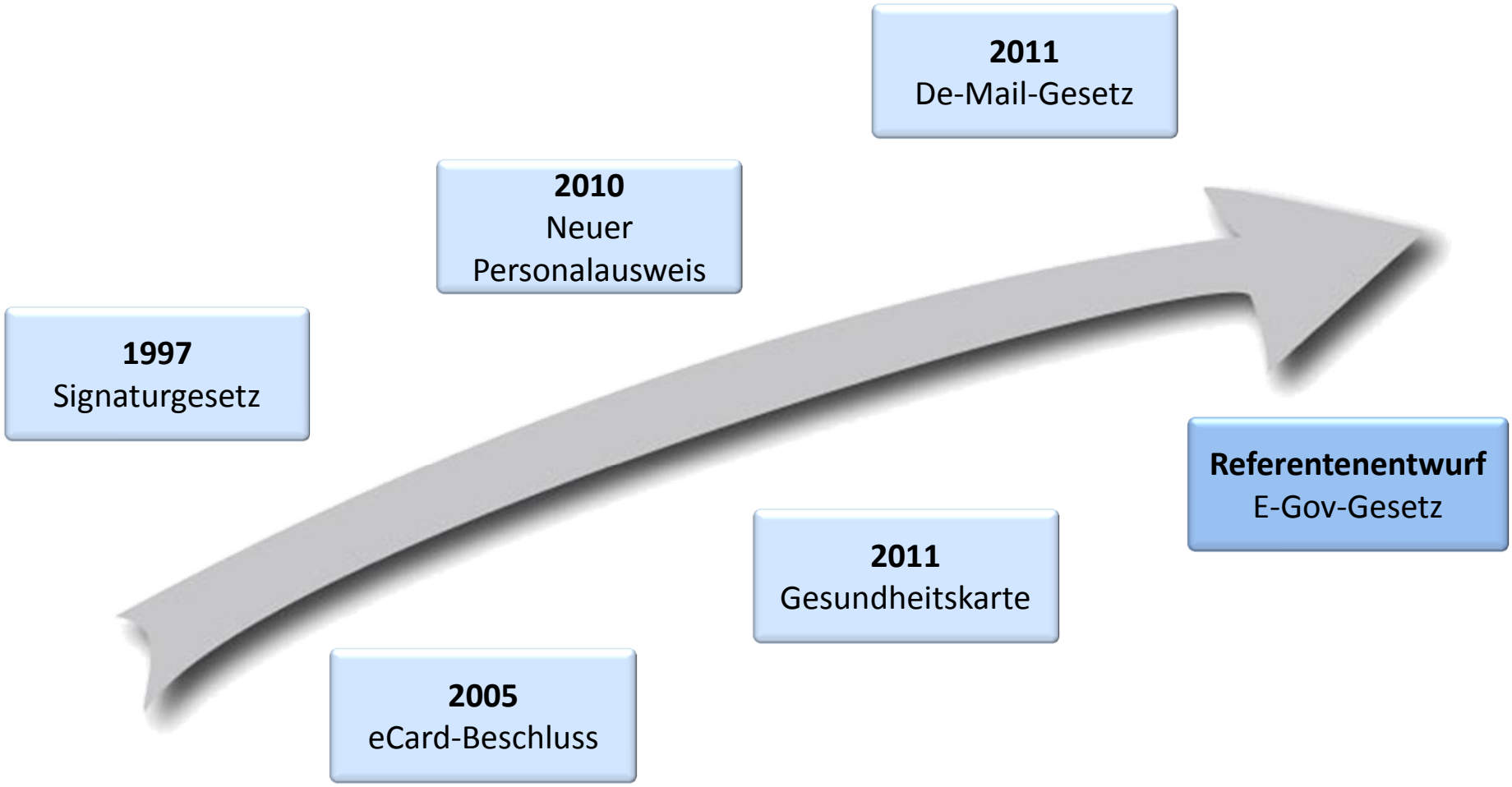
Infrastrukturleistungen des Staates

Andreas Reisen

Leiter des Referates für Pass- und Ausweiswesen,
Identifizierungssysteme
Bundesministerium des Innern

München, 29. März 2012

Beispiele für Infrastrukturleistungen des Staates



Motivation für die Entwicklung von nPA, De-Mail und QES

- **Neuer Personalausweis**
  - Sichere Identitäten als Schlüssel für vertrauenswürdige Aktivitäten im Internet
  - Kryptographie als neues Sicherheitsmerkmal
  - Stärkere Bindung von Dokument und Inhaber durch Biometrie
  - ➢ **Fehlender elektronischer Identitätsnachweis im Netz**
- **De-Mail**
  - E-Mails können mit wenig Aufwand mitgelesen werden
  - Identität der Kommunikationspartner kann nicht nachgewiesen werden
  - Posteingang der Nachricht beim Empfänger kann nicht nachgewiesen werden
  - Sicherheitsfunktionen sind nicht in der Fläche (<5% Verschlüsselung bei E-Mails)
  - ➢ **Der heutigen E-Mail fehlen wichtige Sicherheitsmerkmale**
- **Qualifizierte elektronische Signatur (QES)**
  - Gewährleistung der Integrität und Authentizität von signierten Dokumenten
  - Nicht-Abstreitbarkeit von Erklärungen
  - Perpetuierung
  - ➢ **Rechtssichere elektronische Unterschrift**

nPA: Sicherheitsmerkmale

- Einfaches und sicheres Identifizieren im Internet
  - Kontrolle der Datenfreigabe durch den Ausweisinhaber
- Erhöhte Sicherheit gegenüber der bisherigen Passwortidentifizierung
  - bisher: Passwort oder PIN = nur Wissen
    künftig: Personalausweis + PIN = Besitz + Wissen
- Datenübermittlung nur im Rahmen des Berechtigungszertifikats
  - Berechtigungszertifikat mit Erforderlichkeitsprüfung und Chipüberprüfung
- Einheitliche standardisierte Schnittstelle, verschlüsselte Übertragung
- Nutzung des neuen Ausweises zur gegenseitigen Authentisierung bei Online-Diensten

- **Die Online-Ausweisfunktion bedeutet einen deutlichen Sicherheitsgewinn für den Ausweisinhaber**

De-Mail: Sicherheitsmerkmale

- **Authentizität**
  - Sichere Erst-Registrierung als Vertrauensanker
  - Unterschiedliche Authentisierungsniveaus bei der Anmeldung

    normal: Passwort + Benutzername = nur Wissen
    hoch: Passwort + Benutzername +„Hardware-Token“(z.B. nPA)= Besitz + Wissen
- **Vertraulichkeit**
  - Standard: Transportverschlüsselung zwischen allen Beteiligten
  - Optional: Ende-zu-Ende-Verschlüsselung
- **Nachweisbarkeit**
  - elektronische Versand- und Eingangsbestätigungen („elektronisches Einschreiben“)
  - Integritätsschutz durch qualifizierte elektronische Signatur des De-Mail-Providers
  - Optional: Nutzung von elektronischen Signaturen

- **De-Mail – einfach wie E-Mail, so sicher wie Papierpost**

Potenziale

- **Neuer Personalausweis**
  - Sichere Identifikation auch im Internet möglich (vertrauenswürdige Geschäftsabwicklung)
  - Bürokratieabbau durch medienbruchfreie Prozesse und Dienstleistungen
  - Verhinderung von Identitätsdiebstahl im Internet
  - Altersbeschränkte Dienste möglich – neue Geschäftsfelder
  - Offene Schnittstellen
- **De-Mail**
  - Mehr Breitenwirkung bei grundlegenden Sicherheitsfunktionen (Authentizität, Vertraulichkeit, Nachweisbarkeit)
  - Zunahme medienbruchfreier und automatisierter Abwicklung von Geschäfts- und Verwaltungsprozessen
    → Einfache Integration von De-Mail mit interner E-Mail-Infrastruktur und/oder Fachanwendungen (z.B. ERP-Systeme) über Gateway
- **Qualifizierte elektronische Signatur (QES)**
  - Verlagerung formgebundener konventioneller Prozesse in das Internet
  - Medienbruchfreie Überprüfbarkeit der Urheberschaft und rechtssichere Übermittlung einer Erklärung im elektronischen Datenverkehr

- **nPA, De-Mail und Signatur sind wichtige Sicherheitsinfrastrukturen, die sicheres und selbstbestimmtes Handeln im Netz ermöglichen.**

Aktueller Status

Der neue Personalausweis

- Rund 11,5 Millionen Ausweise ausgegeben
- Durchschnittliche Bearbeitungszeit: ca. sechs Arbeitstage
- 116 erteilte Berechtigungen für neue Dienste
- 82 berechtigte Diensteanbieter (30 aus E-Government, 52 aus E-Business)
- 43 Diensteanbieter sind online
- Rund 500.000 elektronische Aufenthaltstitel (eAT) ausgegeben

De-Mail gestartet

- Gesetzliche Grundlage (De-Mail-Gesetz)
- Voraussetzungen für Akkreditierung als De-Mail-Anbieter geschaffen
- Deutsche Telekom AG, T-Systems und Mentana-Claimsoft GmbH sind akkreditierte De-Mail-Anbieter.

Entwicklungen

Neuer Personalausweis

- Entwicklung von mobilen eID-Applikationen
  - Mobile Authentisierung mit dem neuen Personalausweis (MONA)
  - Sichere elektronische Identifikation mit dem nPA über NFC-fähige Smartphones
  - Prüfung der „Soft-Token-Lösung“ durch BSI
  - „Digital-Handshake“ – Zertifikate mit monatlichem Festpreis
- Zukünftige Entwicklung von Automatenlösungen und SP-Geräten
  - Ausweisfunktion an Fahrtkartenautomaten, etc.
  - Bürgerterminals
  - Cash-Automaten

De-Mail

- United Internet (GMX, WEB.DE, 1&1) wird voraussichtlich im Sommer 2012 akkreditiert
- Deutsche Post AG: Akkreditierung bis Ende 2012 angekündigt

Verantwortung des Staates

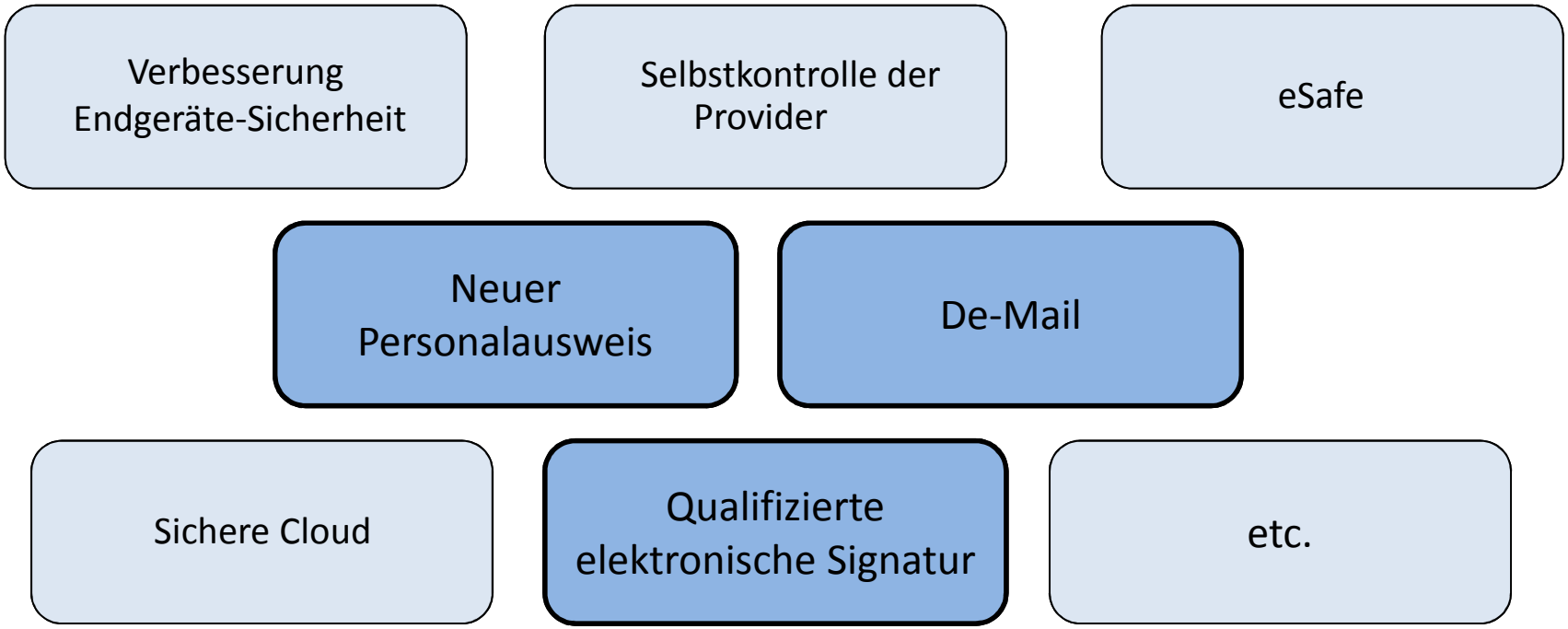
- **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**
  - Ausprägung des allgemeinen Persönlichkeitsrechts durch das Bundesverfassungsgericht im Jahr 2008
  - Schutz persönlicher Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden
  - Das „Handeln im Netz“ muss einfach und sicher sein
  - Gewährleistung einer sicheren Kommunikation
    - Vertraulichkeit
    - Authentizität
  - z.B. Sicherstellung der Anforderungen an die ausgelagerte Datenhaltung
    - Verfügbarkeit
    - Integrität
    - Vertraulichkeit

Selbstbestimmtes Handeln im Netz (SHiNe)

- **Ausgangslage**
  - Immer mehr Vorgänge des alltäglichen Lebens finden im Internet statt
  - Die Bewertung existierender Bedrohungen und eigener Schutzmöglichkeiten ist im Netz deutlich schwieriger als im sonstigen öffentlichen Leben
  - Bürgerinnen und Bürger fühlen sich zunehmend unsicherer im Netz

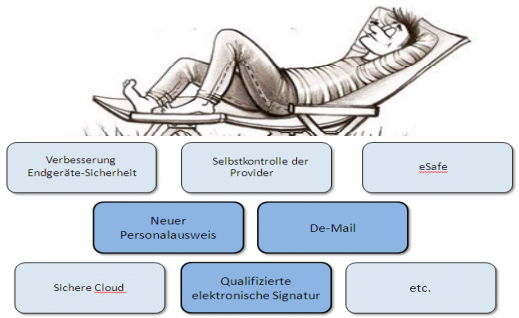
- **Strategie**
  - Verbesserung der IT-Sicherheit der Bürgerinnen und Bürger in ihrem täglichen Handeln im Internet
  - Bewahrung der Selbstbestimmtheit des Einzelnen im Netz angesichts zunehmender Bedrohungen

SHiNe -
Vorhandene und mögliche weitere Bausteine



Blick in die Zukunft

- Der Staat baut rechtliche, organisatorische und technische Hürden ab (z.B. E-Government-Gesetz)
- Bestehende und zusätzlich erforderliche Sicherheitsinfrastrukturen ermöglichen sicheres und selbstbestimmtes Handeln im Internet (neuer Personalausweis, De-Mail, Signatur, etc.)
- Es gibt einen gesellschaftlichen Konsens darüber, dass alle bei der Verbesserung der Sicherheit des Internet zusammenwirken müssen (Staat, Unternehmen, Bürger)
- Ein noch zu entwickelndes „Koordinatensystem“ (Hilfsmittel) soll dazu führen, dass Bürgerinnen und Bürger existierende Bedrohungen und eigene Schutzmöglichkeiten im Netz genauso gut einschätzen können wie im sonstigen öffentlichen Leben.
- **Wichtige Voraussetzungen für selbstbestimmtes Handeln im Netz sind vorhanden.**
- **Nur gemeinsam werden Staat und Wirtschaft die IT-Sicherheit der Bürgerinnen und Bürger im Netz weiter verbessern.**



Weitere Informationen

- **Informationen zum neuen Personalausweis**
  - www.personalausweisportal.de

- **Informationen zu De-Mail**
  - www.de-mail.de

- **Informationen zu technischen Richtlinien des BSI**
  - https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/TRundSchutzprofile/trundschutzprofile_node.html
  - https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Konformitaetsbewertung/Stellen/TR-Liste/TR-Liste_node.html

Vielen Dank!

IT4@bmi.bund.de

www.personalausweisportal.de
www.de-mail.de