BUNDESDRUCKEREI

Der neue Personalausweis – Status und Einsatzszenarien

4. Oktober 2010 I Mark Rüdiger

Agenda

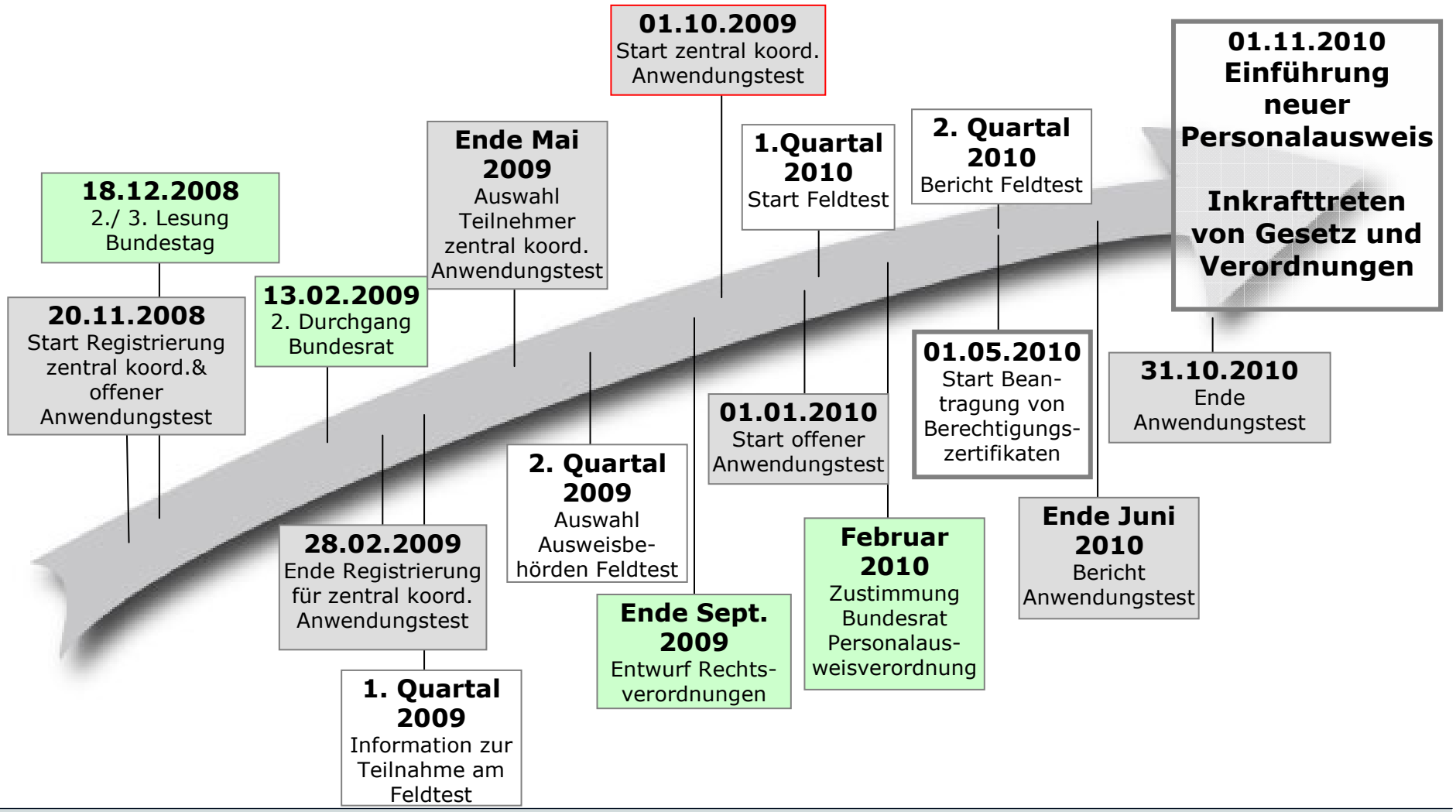
- Zeitplan zur Einführung des neuen Personalausweises (nPA)
- verfügbare Daten des nPA und Anforderungen zur Nutzung
- sicherer Zugriff auf die Daten des nPA
- eID-Service der Bundesdruckerei GmbH
- Aktuelle und zukünftige Einsatz-Szenarien für den neuen Personalausweis

Einführung neuer Personalausweis

- Mit der Einführung des neuen Personalausweises werden die Funktionen des bisherigen Personalausweises um zusätzliche Funktionen ergänzt:

- ePassport: Authentifizierung im hoheitlichen Bereich
- eID: Authentifizierung im E-Business- und E-Government (Lesen von Daten und Alters-/Wohnortvergleich)
- eSign: elektronische Signatur (opt.)

Zeitplan bis zur Einführung



Agenda

- Zeitplan zur Einführung des neuen Personalausweises (nPA)
- verfügbare Daten des nPA und Anforderungen zur Nutzung
- sicherer Zugriff auf die Daten des nPA
- eID-Service der Bundesdruckerei GmbH
- Aktuelle und zukünftige Einsatz-Szenarien für den neuen Personalausweis

Welche Daten stehen zur Verfügung?

- Familienname
- Vornamen
- Doktorgrad
- Tag der Geburt
- Ort der Geburt
- Anschrift
- PLZ (neu)
- Dokumentenart
- Abkürzung „D“ Bundesrepublik Deutschland
- Angabe, ob ein bestimmtes Alter unter oder überschritten wird
- Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht
- Ordensname, Künstlername

Datensparsamkeit

- Alters-/Ortsvergleich
  - Dienstanbieter fragt an, ob Ausweisinhaber älter als ein Vergleichsdatum ist oder in einem bestimmten Bereich wohnt
  - Datum und Adresse werden hierbei nicht ausgelesen
  - nur benötigte Information wird freigegeben

älter als 16 Jahre?

Anforderungen zur eID-Nutzung

- Web-Portal-Betreiber
  - Web-Portal (SSL) unter Einbindung der eID
  - Berechtigungszertifikat (über Antrag beim Bundesverwaltungsamt vom ZDA)
  - eID-Server (Eigenbetrieb) oder eID-Service (Bundesdruckerei-Modell)
  - Übernahme der ID-Daten in eigene Anwendung
  - ggf. Prozessvereinfachung

- Kunde/User
  - neuer Personalausweis
  - AusweisApp (kostenfrei verfügbar)
  - Rechner oder CE mit Internetzugang und Browser
  - Kartenterminal (BSI TR-03119)

Agenda

- Zeitplan zur Einführung des neuen Personalausweises (nPA)
- verfügbare Daten des nPA und Anforderungen zur Nutzung
- sicherer Zugriff auf die Daten des nPA
- eID-Service der Bundesdruckerei GmbH
- Aktuelle und zukünftige Einsatz-Szenarien für den neuen Personalausweis

Schutz vor unberechtigtem Auslesen

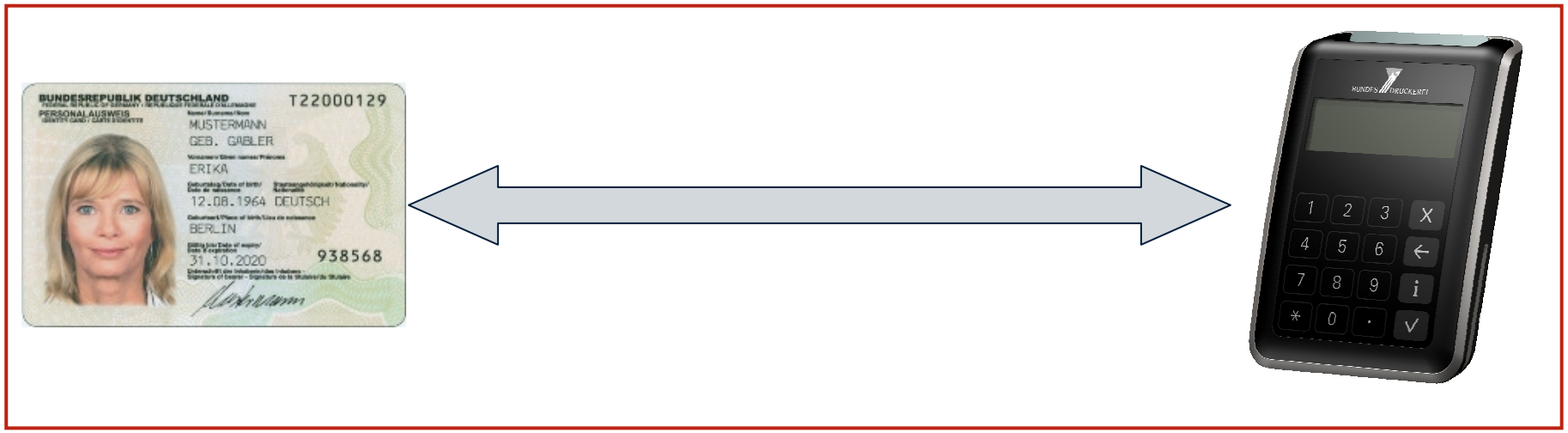
- Password Authenticated Connection Establishment (PACE)
  - durch PIN geschützte Aushandlung eines Schlüssels - ohne Kenntnis der PIN keine Kontaktaufnahme möglich
  - verzögerte PIN-Eingabe - Denial-of-Service gegen PIN ist nicht möglich

Eingabe der PIN

Zugriff auf den Chip

Schutz vor Mithören und Verändern der Kommunikation

- Secure Messaging
  - Aushandeln eines kryptographischen Schlüssels zwischen Lesegerät und Chip mittels PACE und Chip Authentication
  - Schutz von Vertraulichkeit und Authentizität der Kommunikation mit diesen Schlüssel



Schutz vor unberechtigtem Zugriff

- Terminal Authentication
  - Eine Challenge des Chips wird mit dem privaten Schlüssel des Terminals signiert. Der Chip kann diese Signatur mit dem öffentlichen Schlüssel des Terminals verifizieren.
  - Die Authentizität dieses öffentlichen Schlüssels wird durch eine Kette von Zertifikaten bis zu einem während der Personalisierung in den Chip eingebrachten Vertrauensanker sichergestellt.
  - Nur berechtigte Parteien können die Daten lesen, Leserechte können für einzelne Daten erteilt werden

Terminal Authentication

Schutz der Authentizität

- Chip Authentication
  - Bei der Chip Authentication werden mit der Diffie-Hellman-Schlüsselvereinbarung neue Sitzungsschlüssel erstellt.
  - Dabei verwendet der Chip ein statisches Schlüsselpaar, dessen Authentizität durch eine digitale Signatur des öffentlichen Schlüssels geschützt ist. Die Signatur kann mit Hilfe von Zertifikaten im Rahmen der Passive Authentication verifiziert werden.
  - Die Zertifikate für diese Prüfung müssen dem Lesegerät auf authentischem Wege bekannt gemacht werden.

Chip Authentication

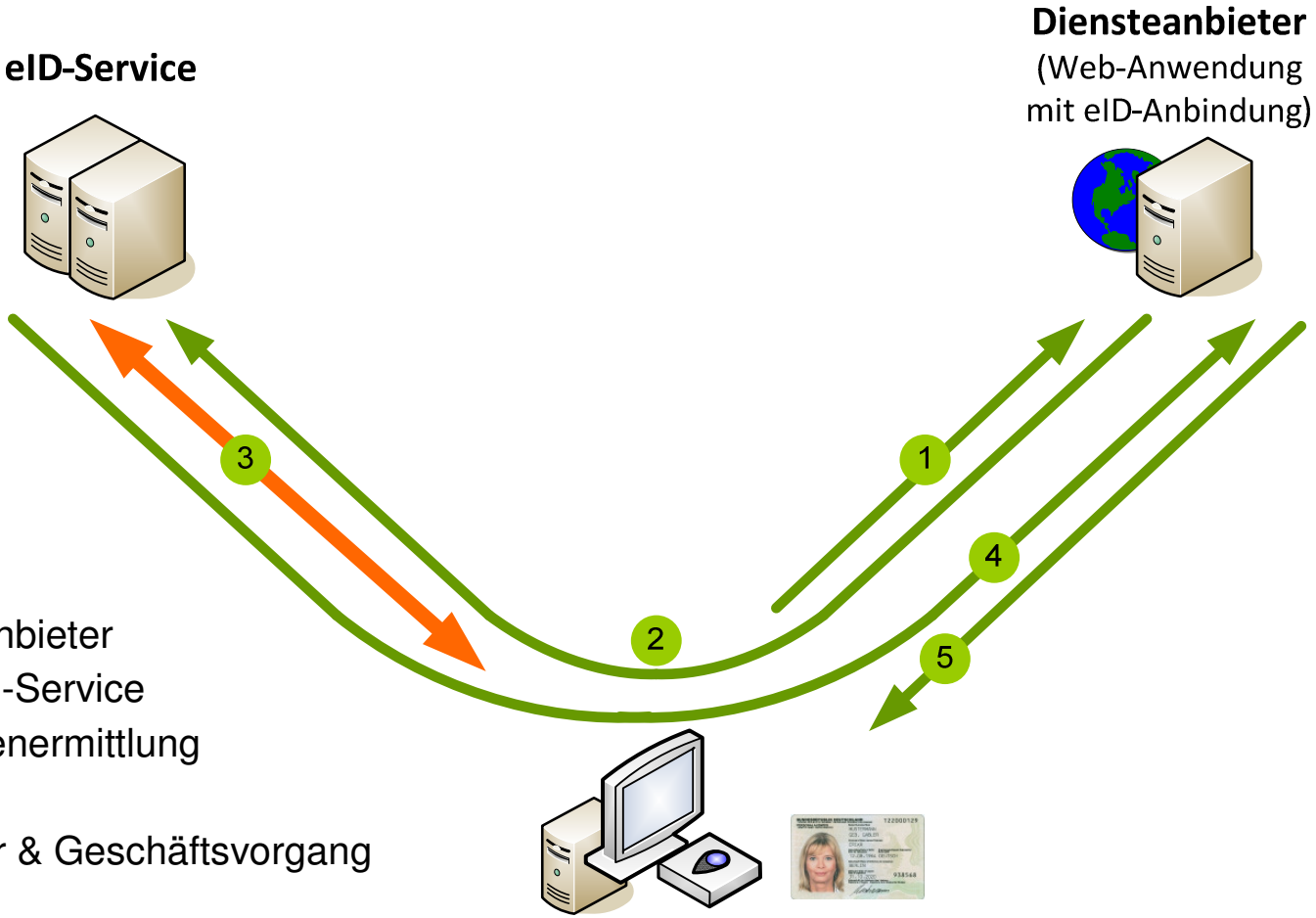
Agenda

- Zeitplan zur Einführung des neuen Personalausweises (nPA)
- verfügbare Daten des nPA und Anforderungen zur Nutzung
- sicherer Zugriff auf die Daten des nPA
- **eID-Service der Bundesdruckerei GmbH**
- Aktuelle und zukünftige Einsatz-Szenarien für den neuen Personalausweis

eID-Service - Übersicht

- eID-Service als Dienstleistung der Bundesdruckerei GmbH
  - eID-Service als vermittelnde Instanz liest im Namen des Diensteanbieter Kundendaten aus dessen nPA aus und stellt diese in verifizierbarer Form zur Verfügung
  - international standardisierte Schnittstelle, SAML-Token
  - eID Service wird vollständig im Hintergrund betrieben
  - keine zusätzlichen Sicherheits-Anforderungen an IT Infrastruktur
  - geringer Integrationsaufwand für Diensteanbieter

eID-Service - Prozessablauf



1: Anfrage beim Dienstanbieter
2: Weiterleitung zum eID-Service
3: Identifikation und Datenermittlung
4: Rückgabe Daten
5: Bestätigung an Bürger & Geschäftsvorgang

Agenda

- Zeitplan zur Einführung des neuen Personalausweises (nPA)
- verfügbare Daten des nPA und Anforderungen zur Nutzung
- sicherer Zugriff auf die Daten des nPA
- eID-Service der Bundesdruckerei GmbH
- Aktuelle und zukünftige Einsatz-Szenarien für den neuen Personalausweis

Einsatz-Szenarien für den neuen Personalausweis

- User-bezogener Content an Endgeräten
  - Computer, Smart Phone, Set-top Box, Hybrid-TV
  - Alterscheck (anonym) oder eindeutige ID verfügbar (GwG- und SigG-Identifizierung)
  - neue Geschäftsmodelle für Content-Provider denkbar
- Digitales Rechtemanagement, fehlende Übertragbarkeit
  - Wechsel der Rechtebindung vom Gerät hin zum Kunden
  - mobile Nutzung der Pay-TV-Lizenz durch Kopplung an nPA
- Nutzung diverser Dienste auf verschiedenen Endgeräten
  - Ablösung diverser accounts durch „Single Sign On“ – immer nPA und PIN
- User-Content verlagert sich ins Netz
  - Sicherer einheitlicher und mobiler Zugriff über verschiedenen Endgeräte
  - Social Web Plattformen
  - Smart Home, Zugriff ins Home-Netz

Vielen Dank für Ihre Aufmerksamkeit

Mark.Ruediger@bdr.de

Tel: 030 2598 1075

www.bundesdruckerei.de