BUNDESDRUCKEREI

Die eID Funktion des neuen Personalausweises

24. Mai 2011 I Mark Rüdiger

Einführung neuer Personalausweis

- Mit dem neuen Personalausweis wurden zusätzliche Funktionen eingeführt:

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

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?

Welche Daten stehen zur Verfügung?

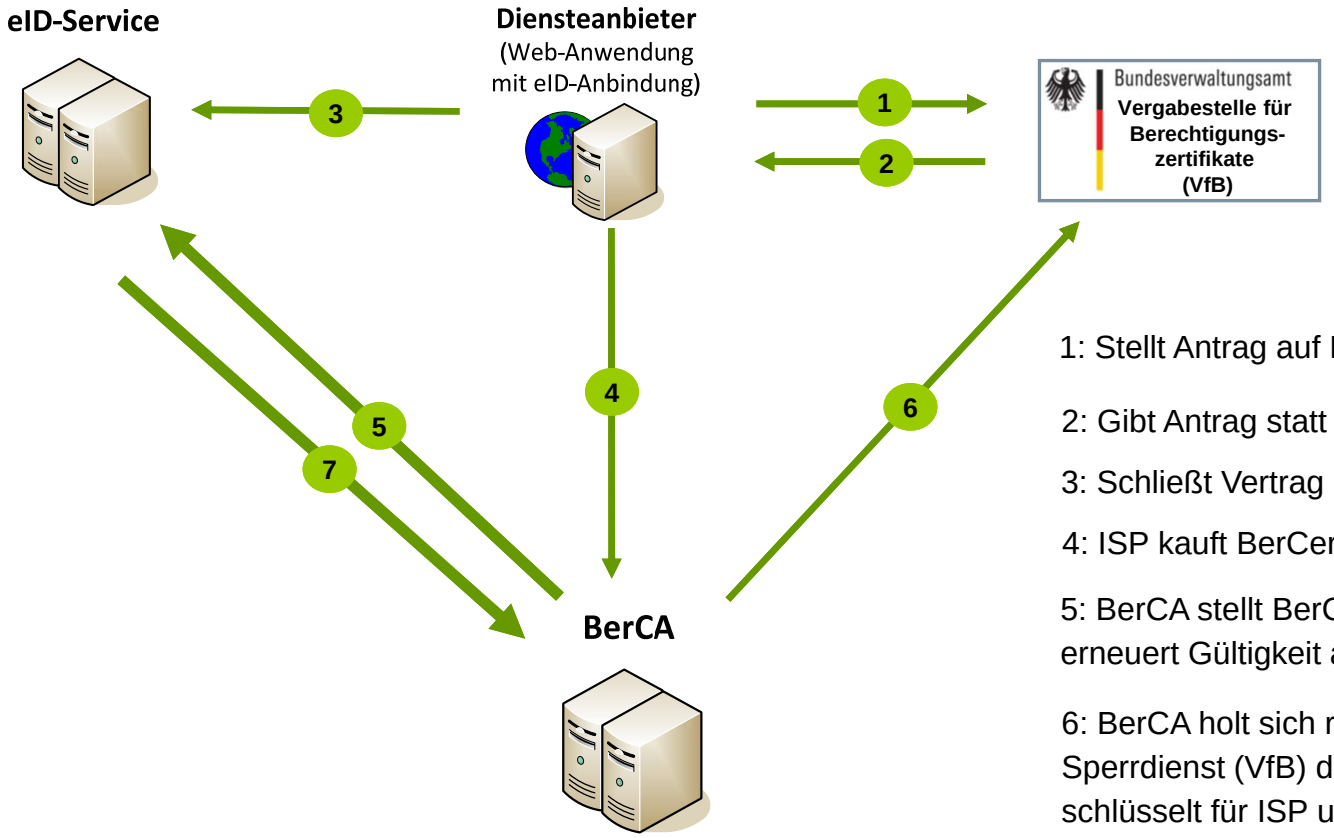
- Familienname
- Vornamen
- Doktorgrad
- Tag der Geburt
- Ort der Geburt
- Anschrift
- PLZ (neu)
- Dokumentenart
- Abkürzung „D“ Bundesrepublik Deutschland
- Angabe, ob ein bestimmtes Alter unter oder überschritten wird
- Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht
- Ordensname, Künstlername

sicherer Zugriff auf die Daten des nPA

BUNDESDRUCKEREI

- Schutz vor unberechtigtem Auslesen - PIN
  - Password Authenticated Connection Establishment (PACE)
- Schutz vor Mithören und Verändern der Kommunikation - Verschlüsselung
  - Secure Messaging
- Schutz vor unberechtigtem Zugriff
  - Terminal Authentication
- Schutz der Authentizität
  - Chip Authentication

Berechtigungszertifikat



1: Stellt Antrag auf BerCert

2: Gibt Antrag statt

3: Schließt Vertrag mit eID SP

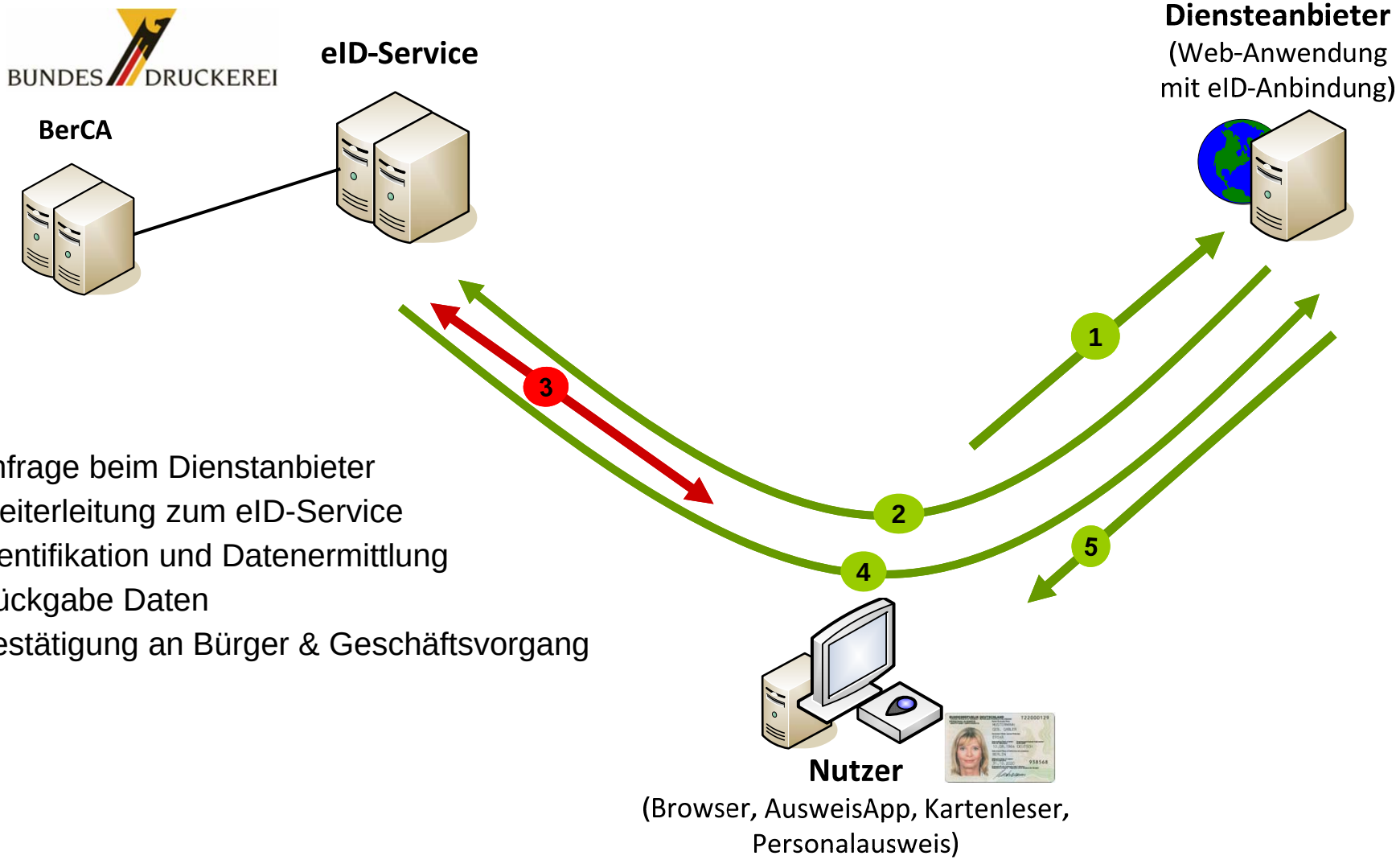
4: ISP kauft BerCert

5: BerCA stellt BerCert dem eID SP zur Verfügung, erneuert Gültigkeit alle 24h

6: BerCA holt sich regelmäßig vom Globalen Sperrdienst (VfB) die Sperrliste (stündlich) BerCA schlüsselt für ISP um

7: BerCA stellt dem eID SP für den ISP umgeschlüsselte Sperrliste regelmäßig zur Verfügung (stündlich), eID SP holt sie ab

eID-Service - Prozessablauf



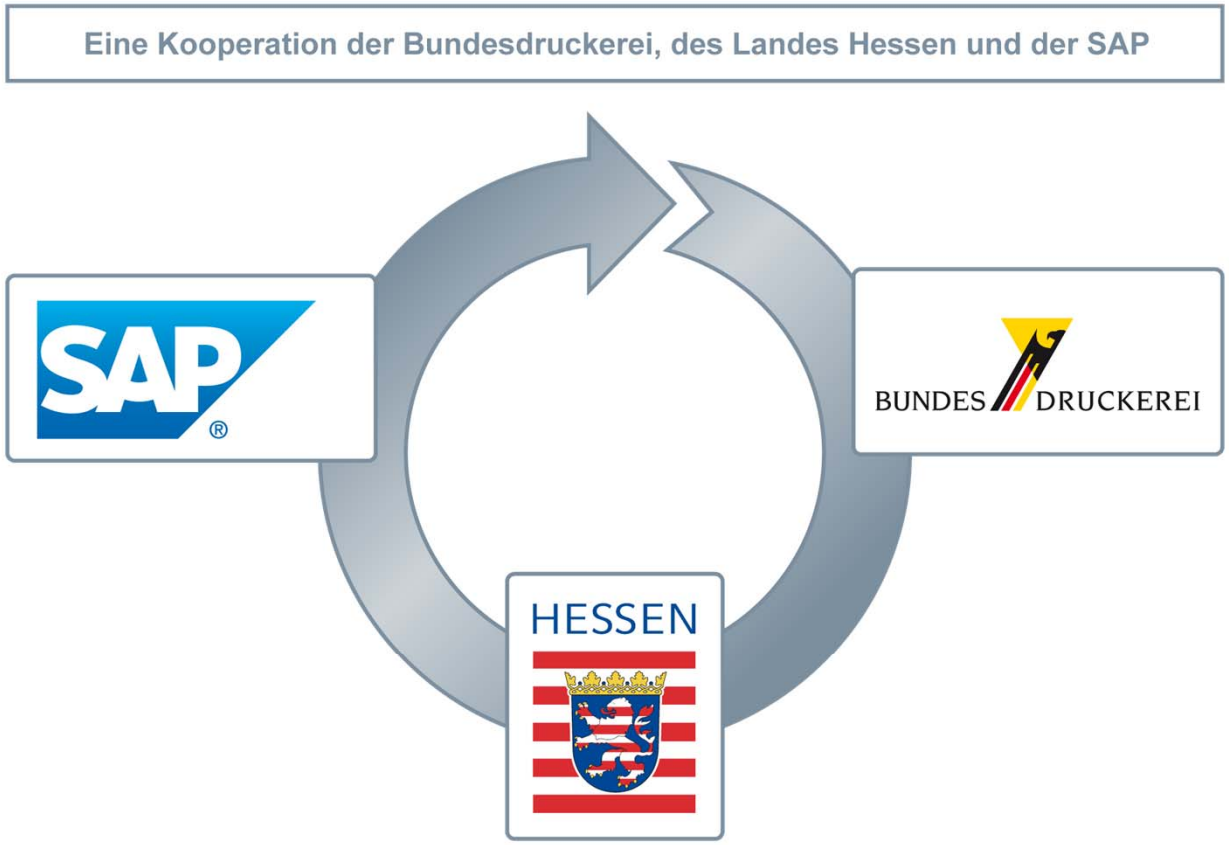
1: Anfrage beim Dienstanbieter
2: Weiterleitung zum eID-Service
3: Identifikation und Datenermittlung
4: Rückgabe Daten
5: Bestätigung an Bürger & Geschäftsvorgang

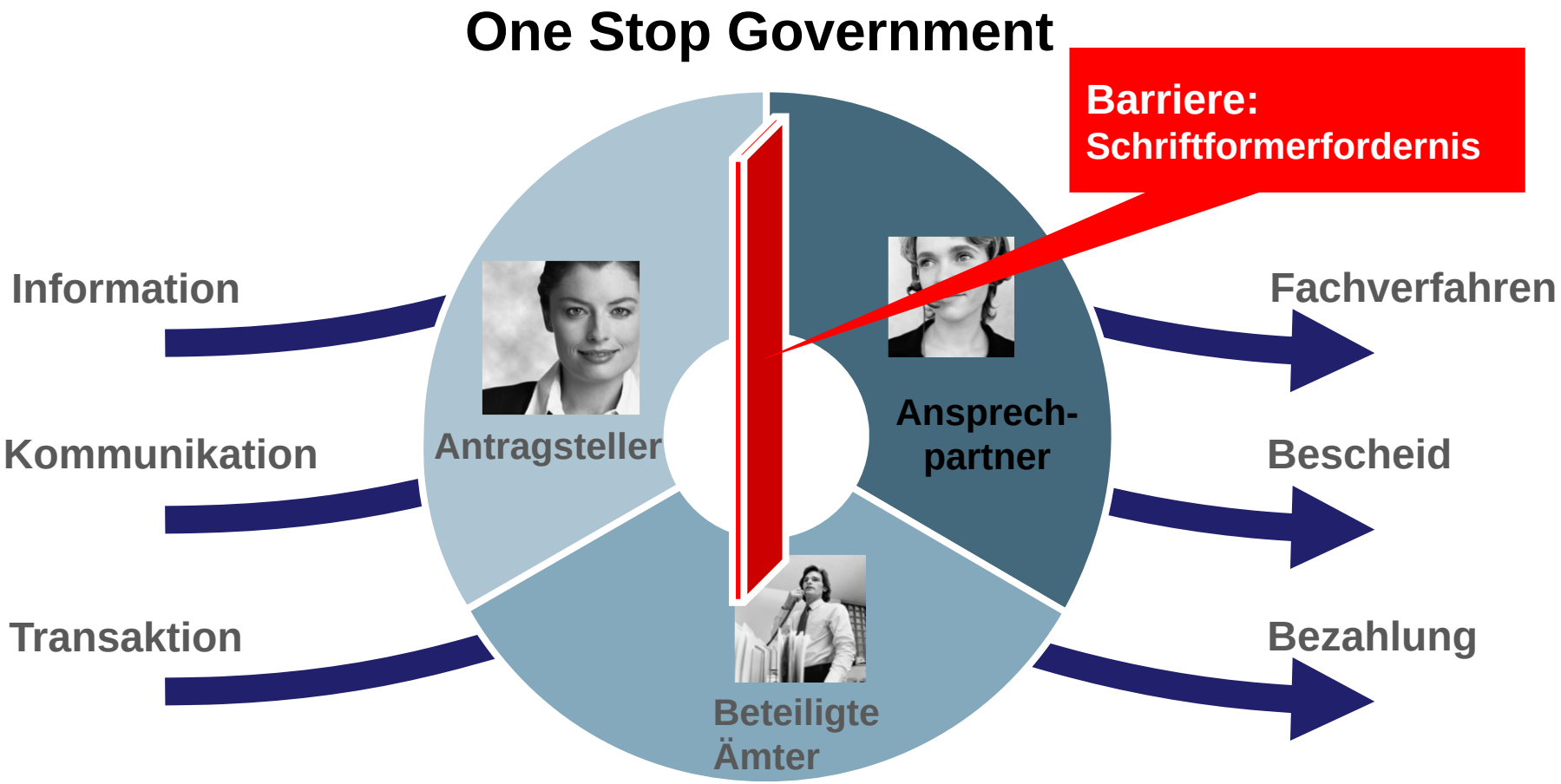
Einsatz-Szenarien für den neuen Personalausweis

BUNDESDRUCKEREI

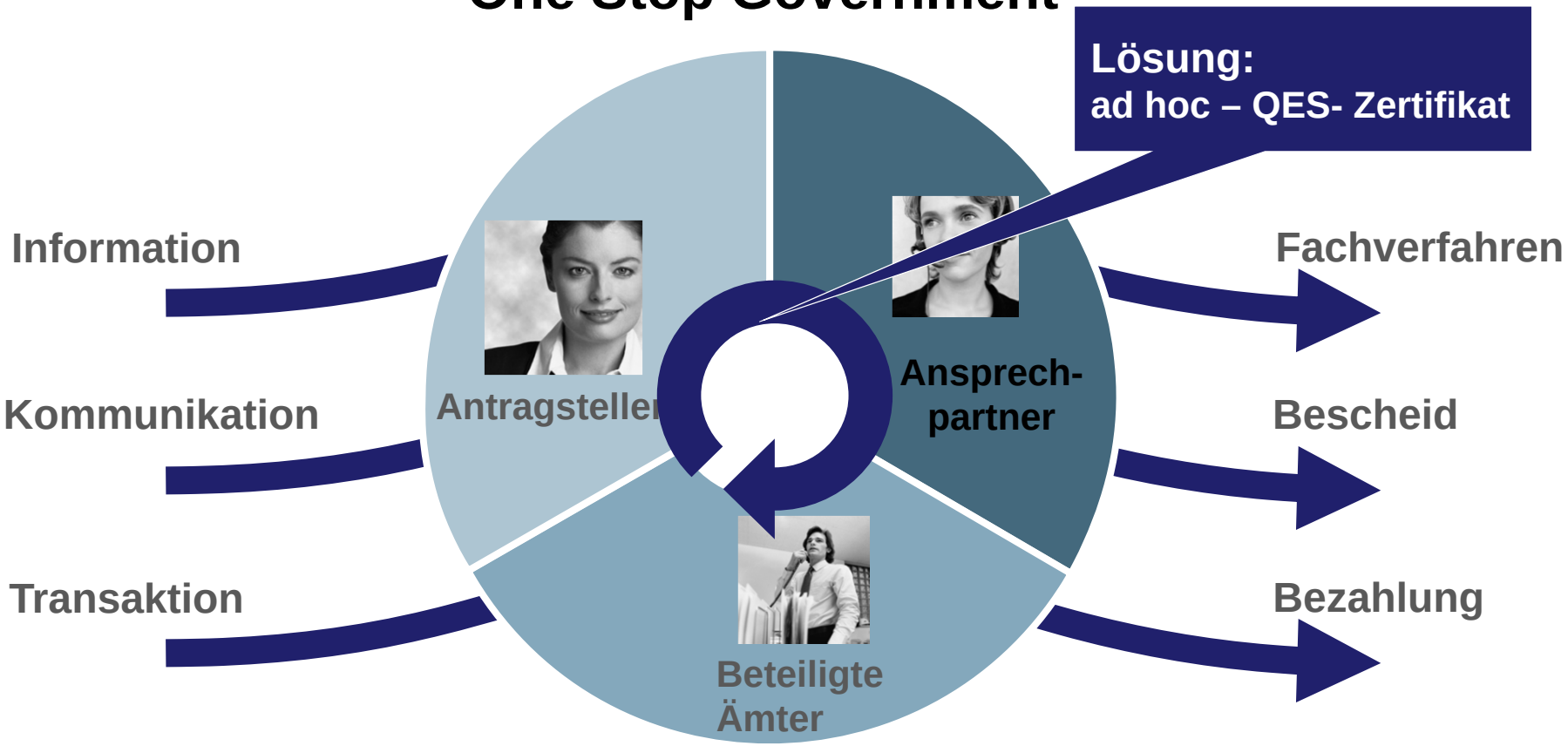
- User-bezogener Content an Endgeräten
  - Computer, Smart Phone, Set-top Box, Hybrid-TV
  - Alterscheck (anonym) oder eindeutige ID verfügbar (GwG- und SigG-Identifizierung)
  - neue Geschäftsmodelle für Content-Provider denkbar
- Digitales Rechtemanagement, fehlende Übertragbarkeit
  - Wechsel der 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

Prototyp ad hoc QES-Zertifikate




One Stop Government
Barriere:
Schriftformerfordernis
Information
Kommunikation
Transaktion
Antragsteller
Ansprech-
partner
Beteiligte
Ämter
Fachverfahren
Bescheid
Bezahlung

One Stop Government

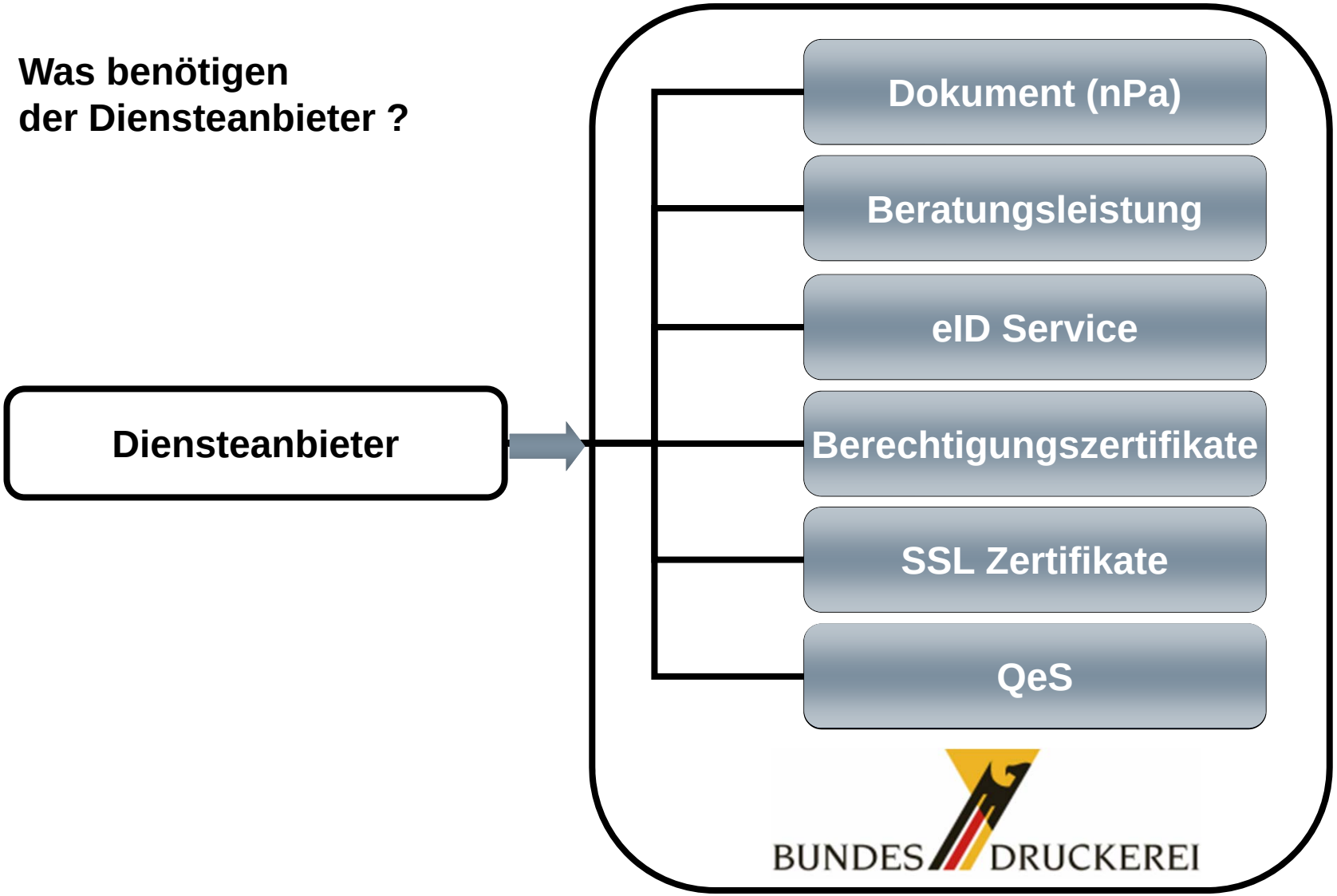


Durchgängige Prozessketten

Ad hoc -Zertifikate, QES mit dem nPA

Full Service ID Provider

Was benötigen der Diensteanbieter ?



Zusammenfassung und Kontakt

- höchste Sicherheit bei einfacher Nutzung
- Kostenlos verfügbare Infrastruktur
- nPA-Daten per XML-SAML-Token zur Weiterverarbeitung
- Bündelung aller Securityprozesse durch Full Service der Bundesdruckerei
- vollständige Integrationsleistung möglich

Mark.Ruediger@bdr.de

Tel: 030 2598 1075

www.bundesdruckerei.de