



Neuer Personalausweis (nPA) für beschleunigte digitale
Geschäftsprozesse:

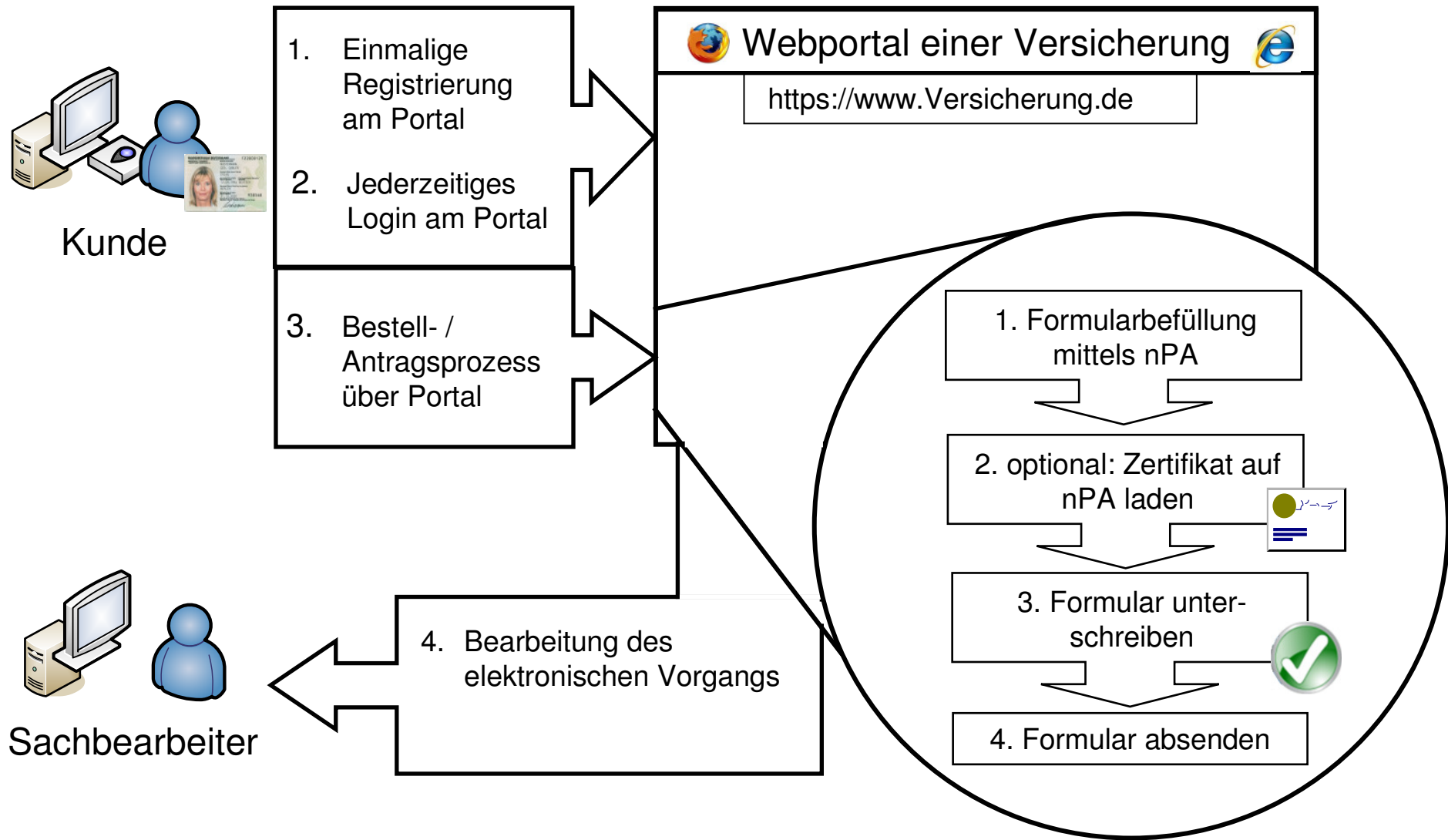
Die „schnelle“ elektronische Signatur mit ad hoc-Zertifikaten

23. September 2011 | Enrico Entschew

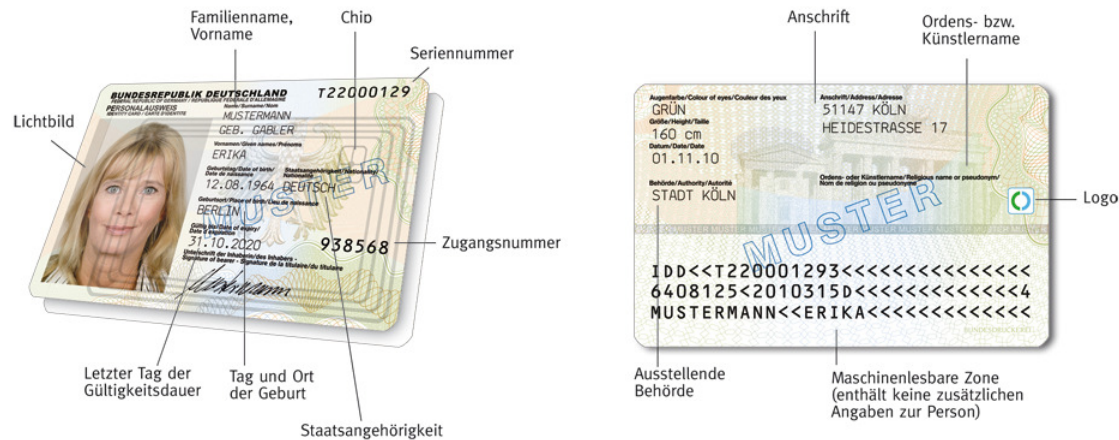
- ▶ Einleitung
- ▶ Vorstellung des neuen Personalausweises
- ▶ Vorstellung der eSign-Funktion
- ▶ Live-Demonstration einer beispielhaften Umsetzung
- ▶ Fazit

- ▶ Sichtausweis: alle Sichtfunktionen des herkömmlichen Personalausweises
- ▶ Nur eine Karte für mehrere Anwendungen → Drei elektronische Funktionen:
 - **ePass** (Anwendung im hoheitlichen Bereich)
 - schneller elektronischer Zugriff auf die Ausweisdaten durch hoheitliche Stellen
 - **eID** (Anwendung für die elektronische Identitätsfunktion im Internet - optional)
 - Online- und Offline-Identifikation
 - Login-Funktion
 - Alters- und Wohnortverifikation etc
 - **eSign** (Anwendung zur Erstellung qualifizierter elektronischer Signaturen - optional)
 - Erzeugung qualifizierter elektronischer Signaturen (QES)

Praktische Anwendung des nPA am Beispiel



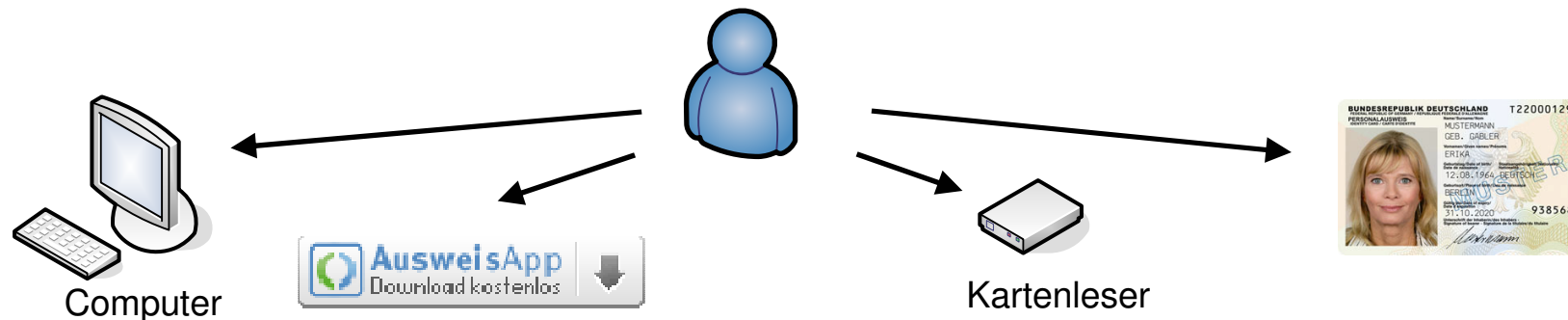
Auslieferungszustand des nPA



- ▶ eID-Funktion eingeschaltet
- ▶ eSign-Funktion nicht aktiviert
- ▶ PIN-Brief ausgegeben
- ▶ Individuelle Zugangsnummer (Card access number – CAN) vorhanden

► Komponenten für **eID- und eSign-Funktion** beim Bürger:

- nPA mit eingeschalteter eID-Funktion und eID-PIN
- Computer (Windows, Mac, Linux)
- Installierter nPA-Kartenleser und AusweisApp



► Komponenten für **eID-Funktion** beim Diensteanbieter:

- eID-Service oder eID-Server
- Berechtigungszertifikat

► Komponenten für **eSign-Funktion** beim Diensteanbieter:

- Anbindung an Trustcenter (zum Bereitstellen der Zertifikate)
- Signaturprüfsoftware (zum Prüfen der Signaturen)

- ▶ **Einzelfunktionen**
 - Ausweisvorbereiten durch Signatur-PIN-Setzen
 - Signaturschlüsselpaar-Erzeugung und Zertifikatsaufbringung durch ZDA auf nPA
 - Signieren
 - Löschen Signaturschlüsselpaar und Signatur-PIN

- ▶ **PIN-Eingabe**
 - PIN-Eingabe pro Einzelsignaturvorgang

- ▶ **Flexible Anwendung des nPA als Signaturerstellungseinheit (SSEE)**
 - volle Kontrolle durch den Bürger
 - direkte Übertragung des Zertifikats auf den Personalausweis
 - Löschung und Neugenerierung des Signaturschlüsselpaars durch den Bürger jederzeit möglich
 - Zertifikatslaufzeiten < 1 Jahr denkbar
 - alle bisherigen Vorteile der Einbindung von qualifizierten elektronischen Signaturen in Geschäftsprozessen bleiben voll erhalten

Mit dem nPA sind erstmalig ad hoc-Zertifikate möglich!

- ▶ Eigenschaft
 - Qualifiziertes Zertifikat gemäß Signaturgesetz

- ▶ Vorteile des ad hoc-Zertifikat
 - sofortige Nutzungsmöglichkeit

 - individuelle Zertifikatslaufzeiten möglich

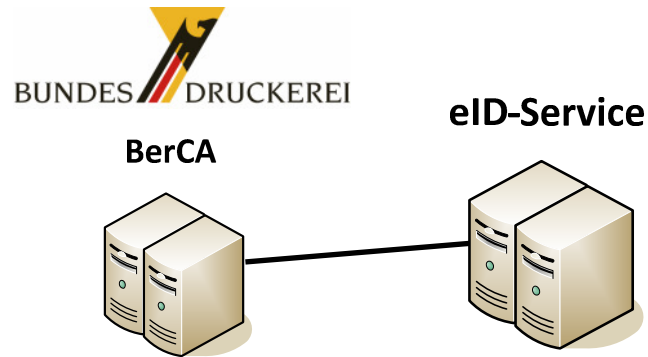
 - Übernahmemöglichkeit der Zertifikatskosten durch den Portalbetreiber (Nutznießer der Signatur)

- ▶ Löschen eines eventuell vorhandenen Signaturschlüsselpaares und Setzen individueller Signatur-PIN
 - Nutzung Komfortkartenleser
 - Setzen der Signatur-PIN

- ▶ Online-Antragsprozess beim ZDA
 - Aufruf der Antragsseite
 - Auswahl des gewünschten Zertifikats
 - Entscheidung über Zertifikatsveröffentlichung, Eingabe Sperrkennwort
 - Erklärungen

- ▶ Start des Aktivierungsprozesses mittels eID-Funktion

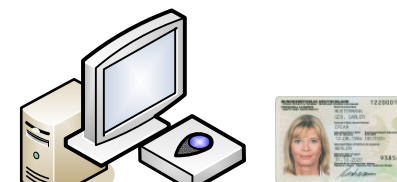
eID-Service und Nachlanden der QES



Trustcenter



- 1: Anfrage bei der D- TRUST (Zertifizierungsdienstanbieter)
- 2: Weiterleitung zum eID-Service
- 3: Identifikation und Datenermittlung
- 4: Rückgabe Daten
- 5: Bestätigung an Bürger & Download des qualifizierten Zertifikates (via eID-Service)

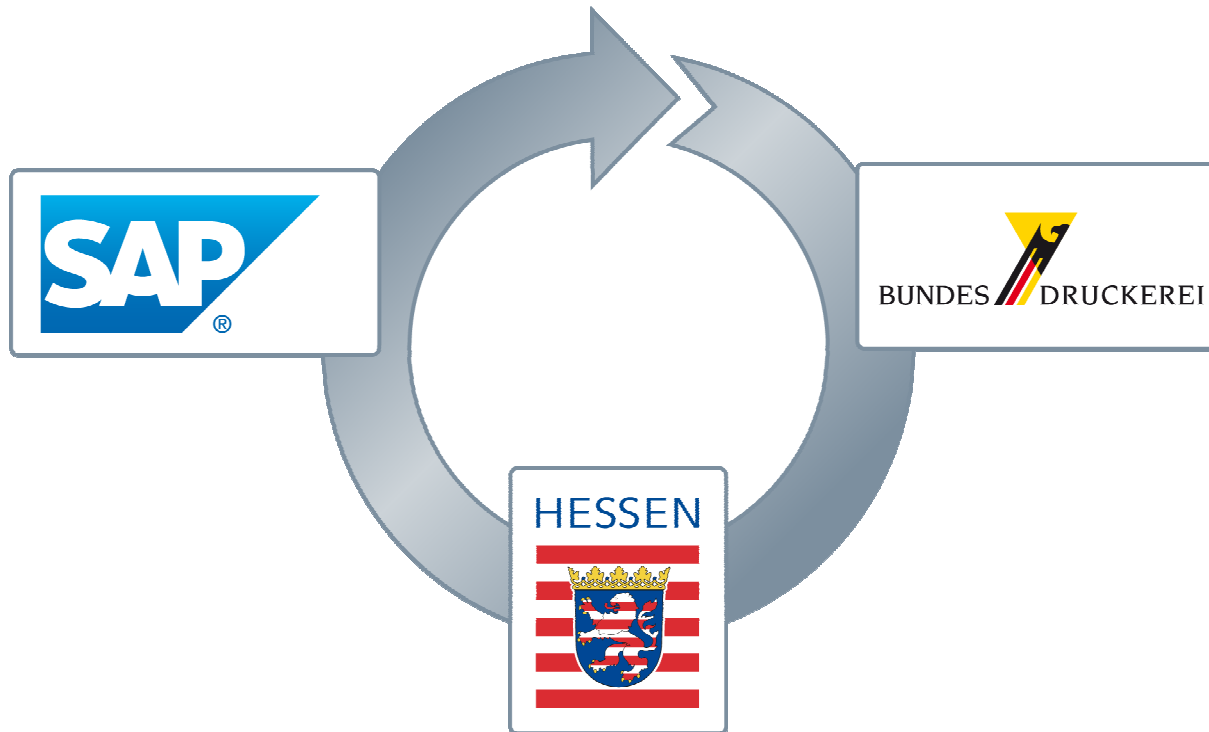


Nutzer

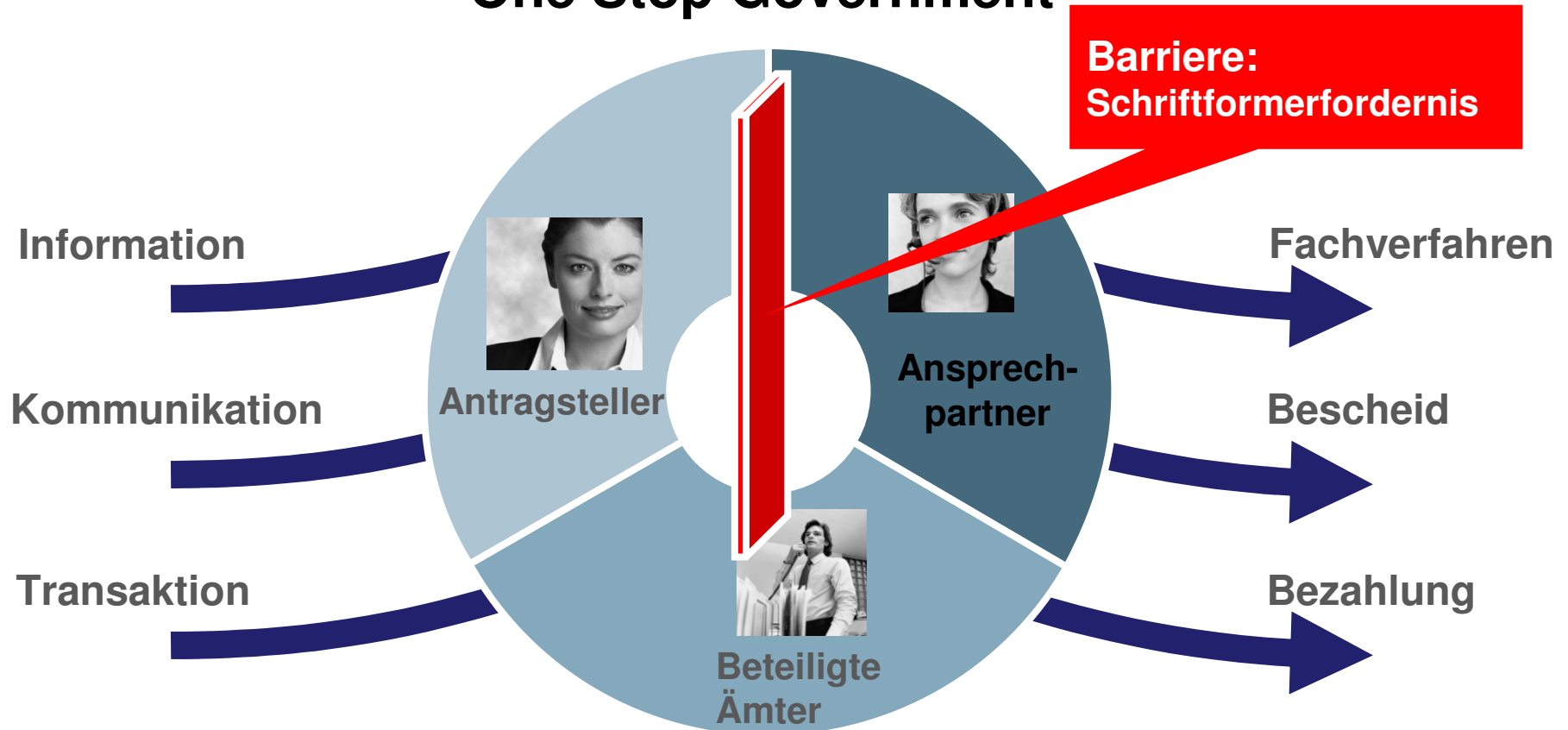
(Browser, Bürgerclient, Kartenleser, Personalausweis)

Prototyp ad hoc-Zertifikate

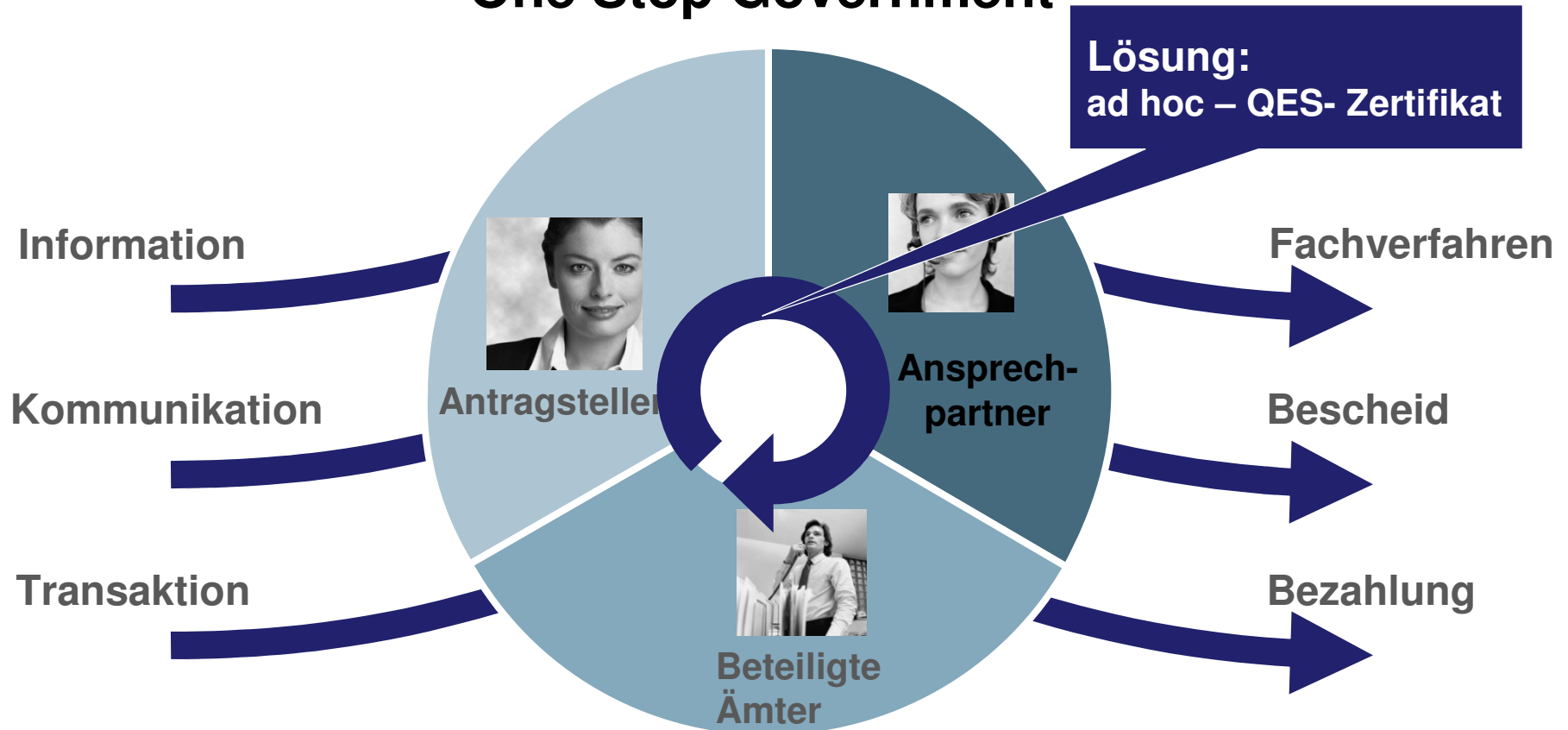
Eine Kooperation der Bundesdruckerei, des Landes Hessen und der SAP



One Stop Government



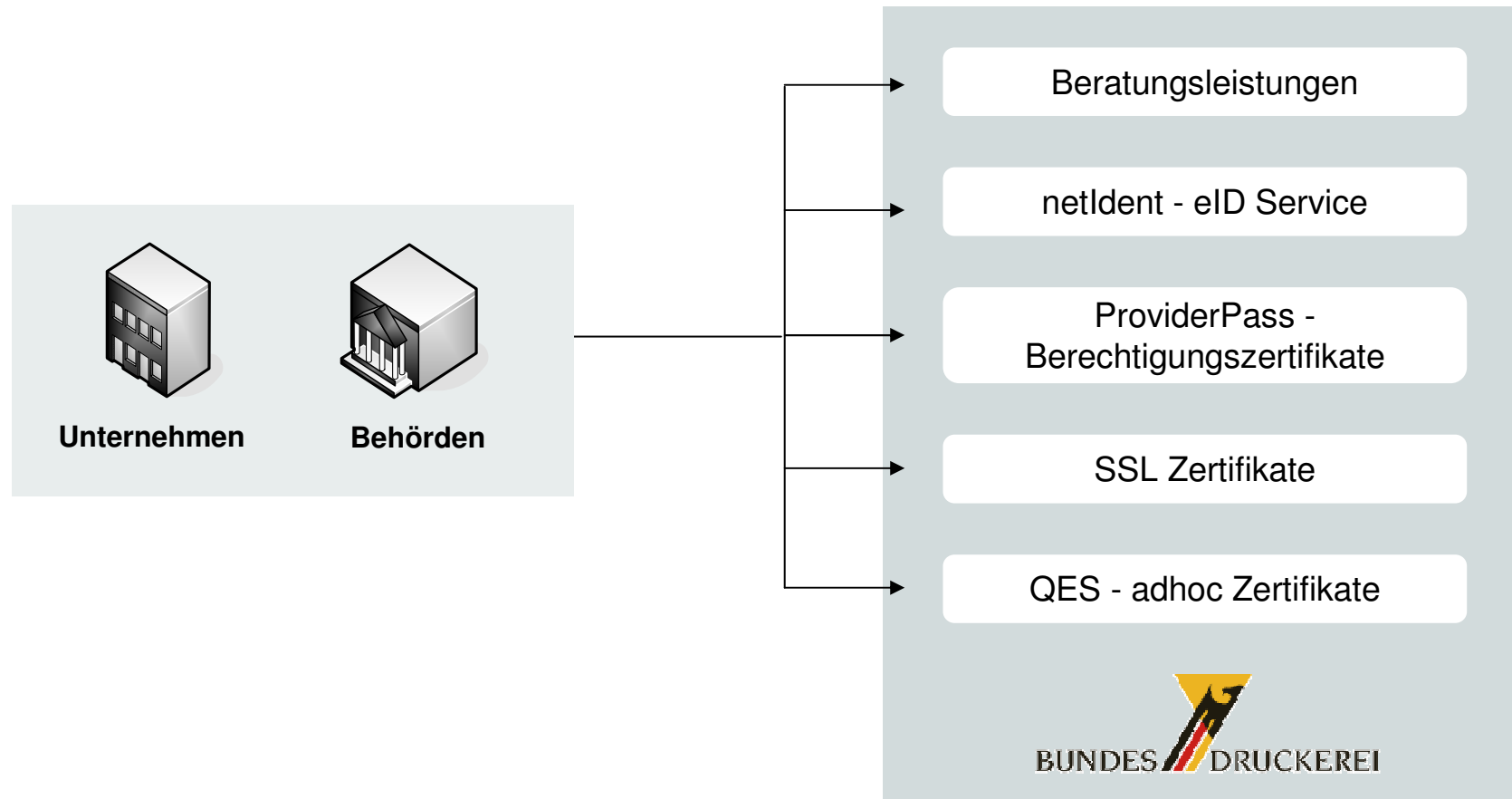
One Stop Government



Durchgängige Prozessketten

- ▶ Das Verfahren ermöglicht erstmalig eine zeitnahe Bereitstellung qualifizierter Zertifikate für elektronische Geschäfts- und Verwaltungsprozesse im Rahmen selbiger.
- ▶ Die Signaturfunktion des nPA kann vollumfänglich im Rahmen der Laufzeit des Personalausweises genutzt werden.
- ▶ Das Verfahren ist sicher, nutzt die bekannten Mechanismen der eID-Funktion und internationaler Standards.
- ▶ Die Benutzerakzeptanz kann durch eine Umkehrung des Bezahlmodells befördert werden.
- ▶ Das Verfahren ist sowohl für Wirtschaft und Verwaltung attraktiv, da die Anzahl der Dokumentenbesitzer kontinuierlich steigt.

Die Bundesdruckerei als Full Service eID-Anbieter



Nur bei der Bundesdruckerei können Unternehmen und Behörden sämtliche benötigten Dienstleistungen und Produkte im Umfeld des neuen Personalausweises aus einer Hand erwerben.

Vielen Dank

Enrico Entschew

Bundesdruckerei GmbH

Oranienstraße 91 | D-10958 Berlin

Internet: www.bundesdruckerei.de

e-mail: enrico.entschew@bdr.de

phone: +49 30 2598-3070