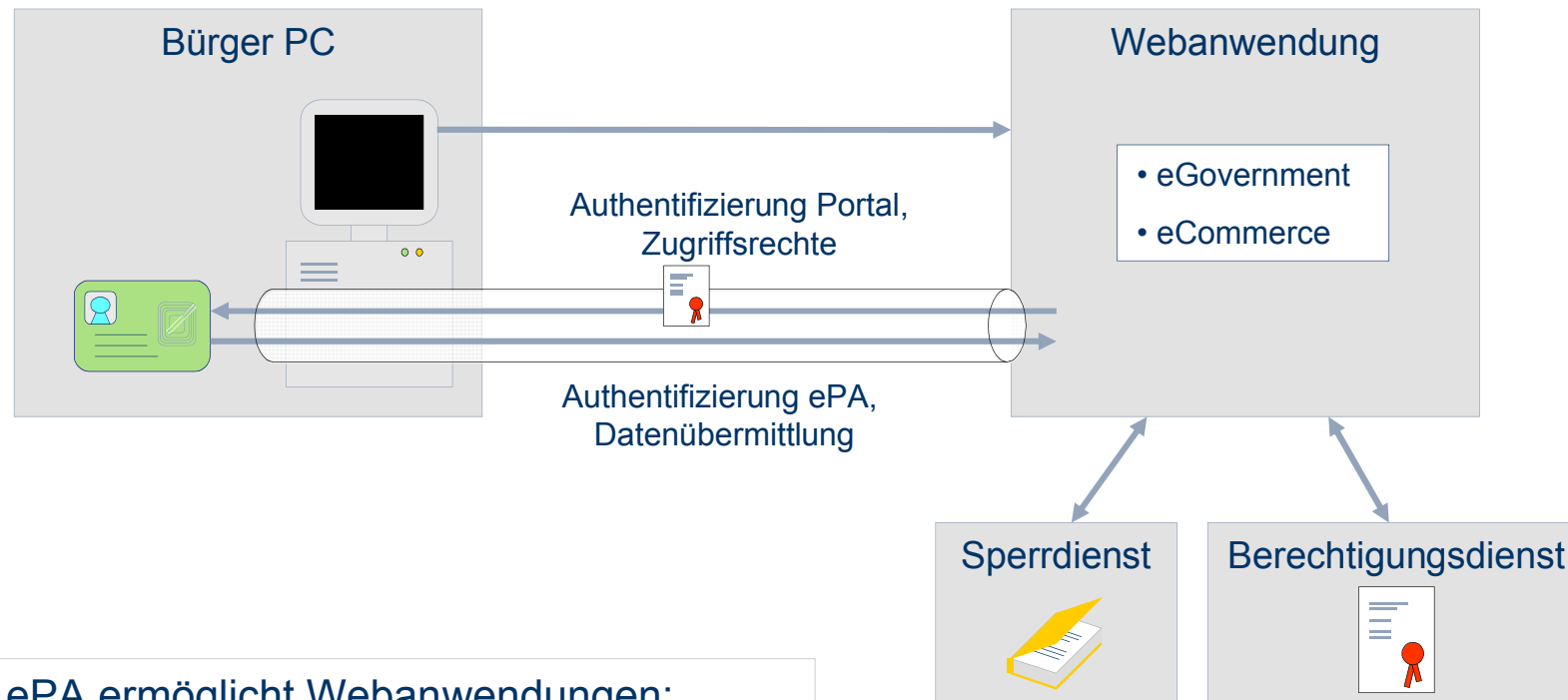


Komponenten und Prozesse bei Ausgabe und Nutzung des elektronischen Personalausweises (ePA)

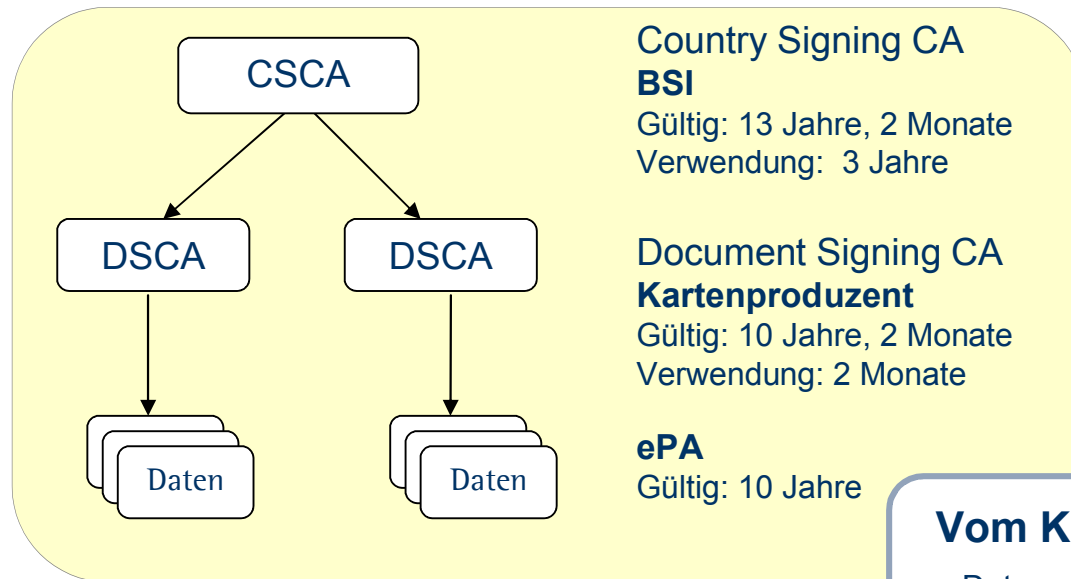


Andrea Klenk, media transfer AG
a-i3/BSI Symposium
23.03.2009



ePA ermöglicht Webanwendungen:

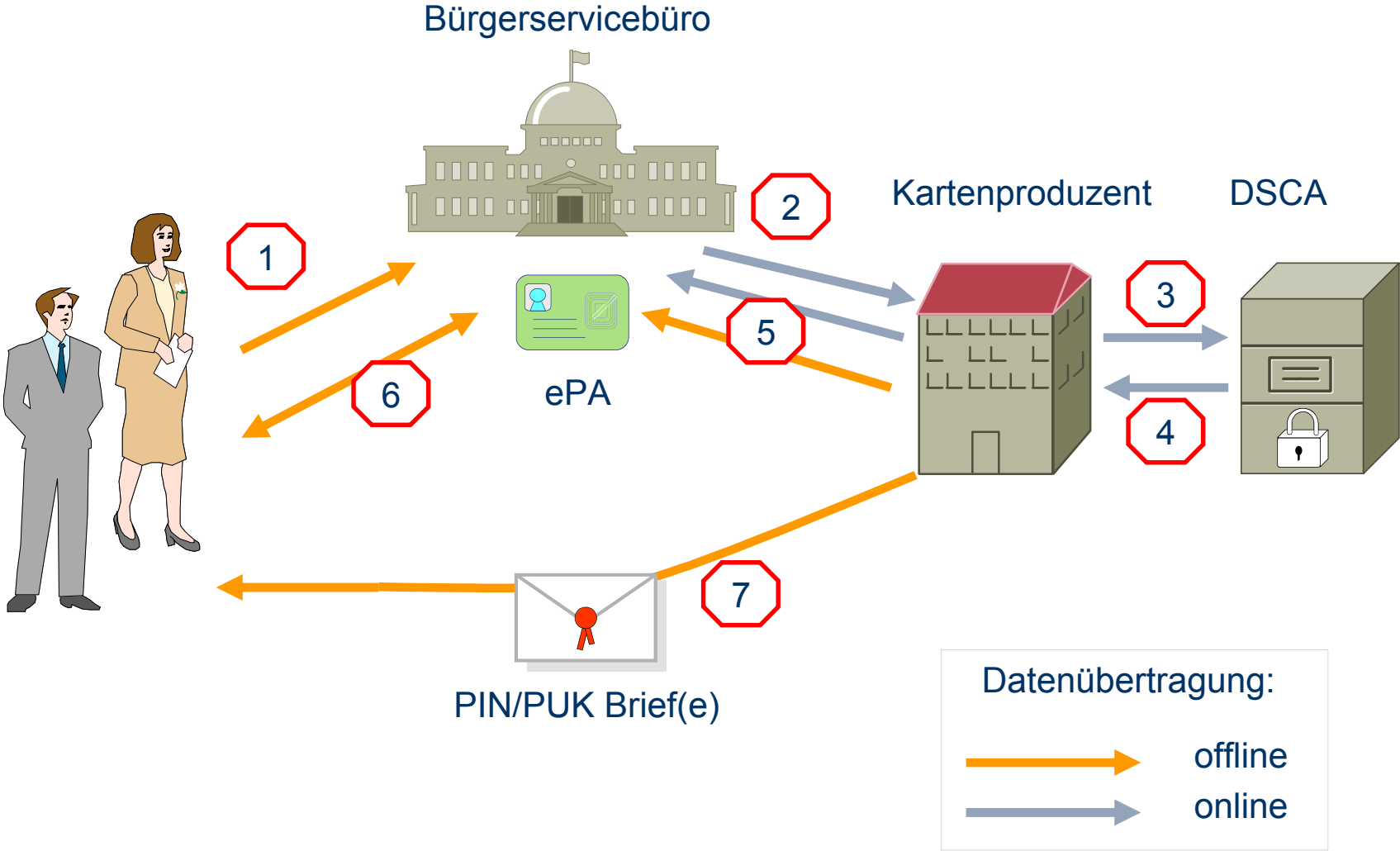
- Registrierung von Personen
- zuverlässige Identifizierung
- starke Authentifizierung



Vom Kartenproduzenten erzeugte Daten:

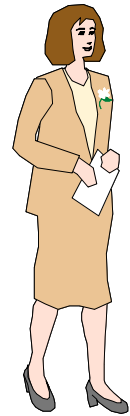
- Datengruppen für ePass
 - MRZ
 - Biometrische Merkmale (Gesicht, Fingerabdruck)
 - Schlüssel zur Authentifizierung
 - ...
- Datengruppen für eID
 - Vor-, Nachname, Künstlername, Titel
 - Adresse, Geburtsdatum / -ort
 - Nationalität, Geschlecht
 - Gültig bis
 - ...
- PIN, CAN, PUK
- Schlüssel für Authentifizierungs-Protokolle
- von DSCA signierte Sicherheitsobjekte
- ...

Ausgabe des ePA

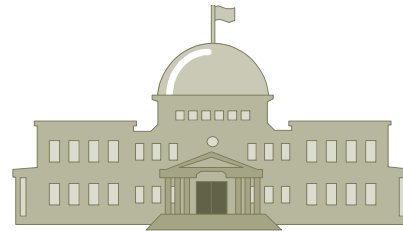


Gültigkeit des ePA : Sperrdienst

Sperrprozess



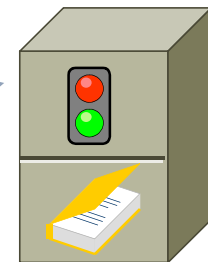
Bürgerservicebüro



Sperrung

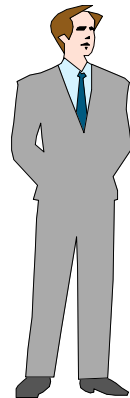


Sperrdienst

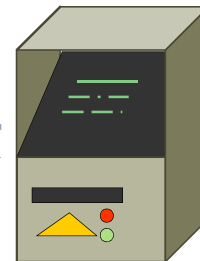


Gültigkeitsprüfung

Datenänderung



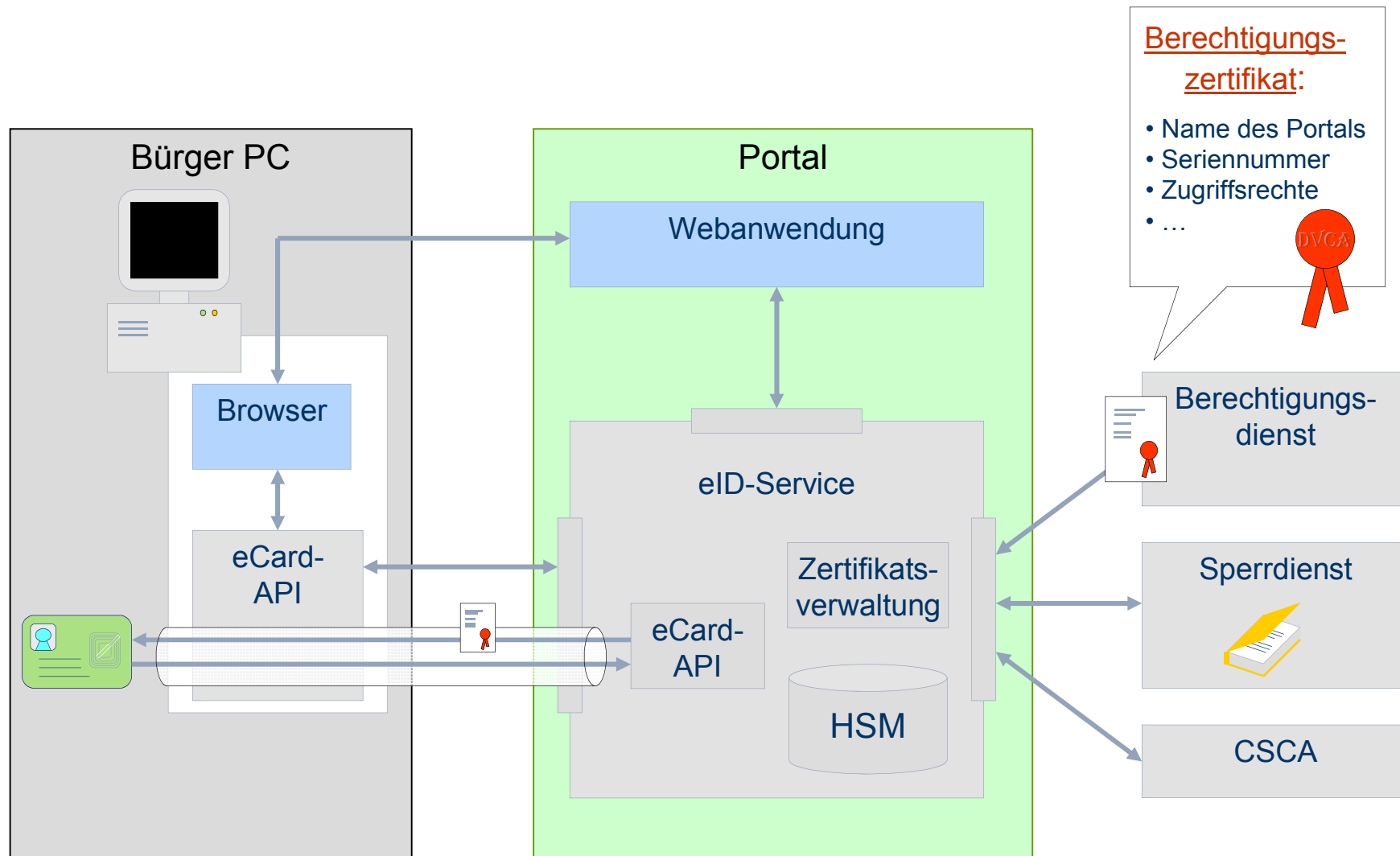
Terminal



Gültigkeitsabfrage



Zugriff auf den ePA: eID Service



Zugriffsrechte: Berechtigungsdienst



Jeweils eine Hierarchie von CV Zertifikaten für

- hoheitliche Anwendungen
- eID Anwendungen (eCom, eGov, Bürgerbüro)
- Anwendungen für qualifizierte Signaturen

- Ziel des Berechtigungsdienstes:
 - verlässliche Authentisierung der Anwendung gegenüber dem Bürger bzw. ePA
 - Vergabe der konkreten Zugriffsrechte
- Berechtigungsdienste stehen in der Verantwortung einer staatlichen Stelle
- Trust Center als Betreiber denkbar
- Vorgabe einer Policy
- Sperrprozess technisch nicht sinnvoll → kurze Gültigkeit der Berechtigungszertifikate
- CA-Zertifikate haben ebenfalls relativ kurze Laufzeiten

ePA Anwendungen und Zugriffsrechte

Kontext	Inhalt	Zugriffsrechte	
		Hoheitl. Anwendung	eCom, eGov
ePass	• MRZ	lesend	-
	• Gesichtsbild (optisch)	lesend	-
	• Fingerabdrücke (optisch)	lesend (*)	-
	• Öffentliche Schlüssel zur Authentifizierung	lesend	-
eID	• Dokumententyp	lesend (*)	lesend (*)
	• Ausgebender Staat	lesend (*)	lesend (*)
	• Ende der Gültigkeit	lesend (*)	lesend (*)
	• Vorname(n), Nachname(n)	lesend (*)	lesend (*)
	• Künstlername	lesend (*)	lesend (*)
	• Akademischer Titel	lesend (*)	lesend (*)
	• Geburtsdatum, Geburtsort	lesend (*)	lesend (*)
	• Nationalität	lesend (*)	lesend (*)
	• Geschlecht	lesend (*)	lesend (*)
	• Adresse	lesend (*) / schreibend (**)	lesend (*)
	• Gemeindekennzahl	lesend (*) / schreibend (**)	lesend (*)
• Aufenthaltserlaubnis	lesend (*) / schreibend (**)	lesend (*)	

(*) = durch Berechtigungszertifikat festgelegt

(**) = nur Bürgerservicebüro

- Entspricht eID Service einem Identity Management System (IDM)?
 - IDM umfasst Speicherung und Verwaltung von Identitäten und Attributen
 - IDM umfasst eine Rollen- und Rechtezuweisung (Autorisierung)
 - IDM umfasst Datenabgleich und Synchronisation versch. Systeme (z.B. Verzeichnisse, Access Management, Datenbanken etc.)
- ⇒ Fazit: eID Service ist eine Teilkomponente, die in ein IDM integriert werden kann.

- Sind PKI Zertifikatsdienste nun überflüssig?
 - nur anwendbar für Identitäten von natürlichen Personen
 - Attribute der Identitäten sind nicht flexibel erweiterbar
 - Geräte-, Provider-, Card-to-Card Prozesse nicht abgedeckt
 - Vielzahl von Protokollen verlangt X.509 Zertifikate (z.B. SMIME, SCEP, SOA Security, Web Service Security, Win/Linux Logon)
- ⇒ Fazit: PKI Dienste (X.509/CV) werden weiterhin benötigt.

- eID Funktionalität des ePA erlaubt:
 - persönliche Registrierung
 - anonyme Registrierung
 - Identifizierung
 - starke Authentifizierung
- Vorteile für Diensteanbieter:
 - erstmals zuverlässige persönliche Online-Registrierung möglich
 - Face-to-Face Kontrolle durch das Bürgerservicebüro
 - teure und nicht-onlinefähige Verfahren wie Post-Ident entfallen
 - sicheres Token und Client Software ohne Kosten für die Diensteanbieter
- Vorteile für Bürger:
 - zuverlässige Authentisierung des Diensteanbieters durch staatl. Zertifikat
 - Anonyme/pseudonyme Verfahren möglich
 - Sicherheit durch evaluierte Komponenten
- Nachteile für Diensteanbieter:
 - Nationales Verfahren, nur für deutsche Bürger
 - Diensteanbieter sind abhängig von Verfügbarkeit, Handhabbarkeit und Performanz der Client Komponenten
 - Zusätzliche Zertifikate werden trotzdem benötigt

Andrea Klenk

media transfer AG (mtG)

Dolivostraße 11

64293 Darmstadt

www.mtg.de

Tel. 06151 819313

aklenk@mtg.de