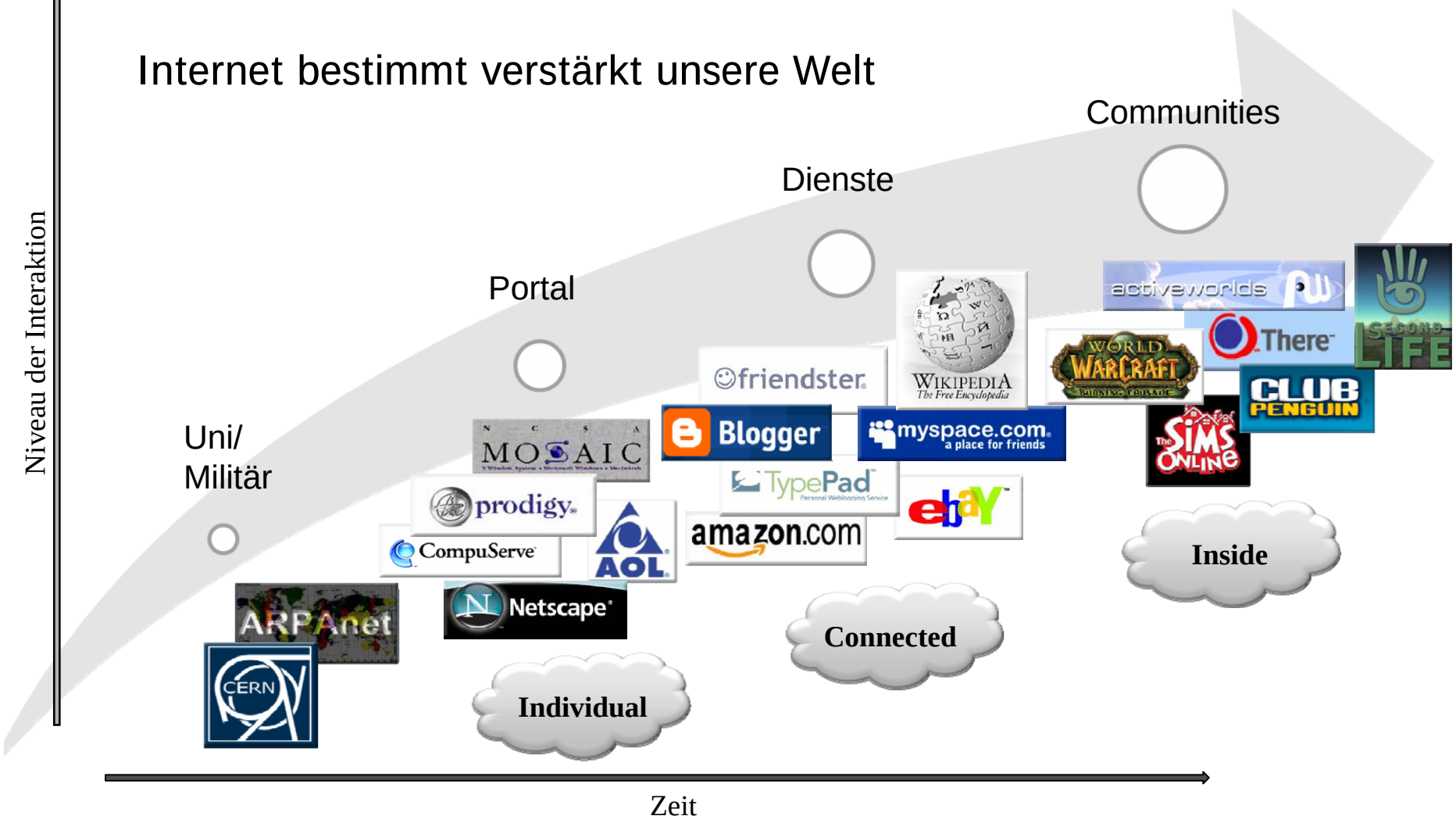
Eine sichere Welt im Internet – der neue Personalausweis

Jens Fromm

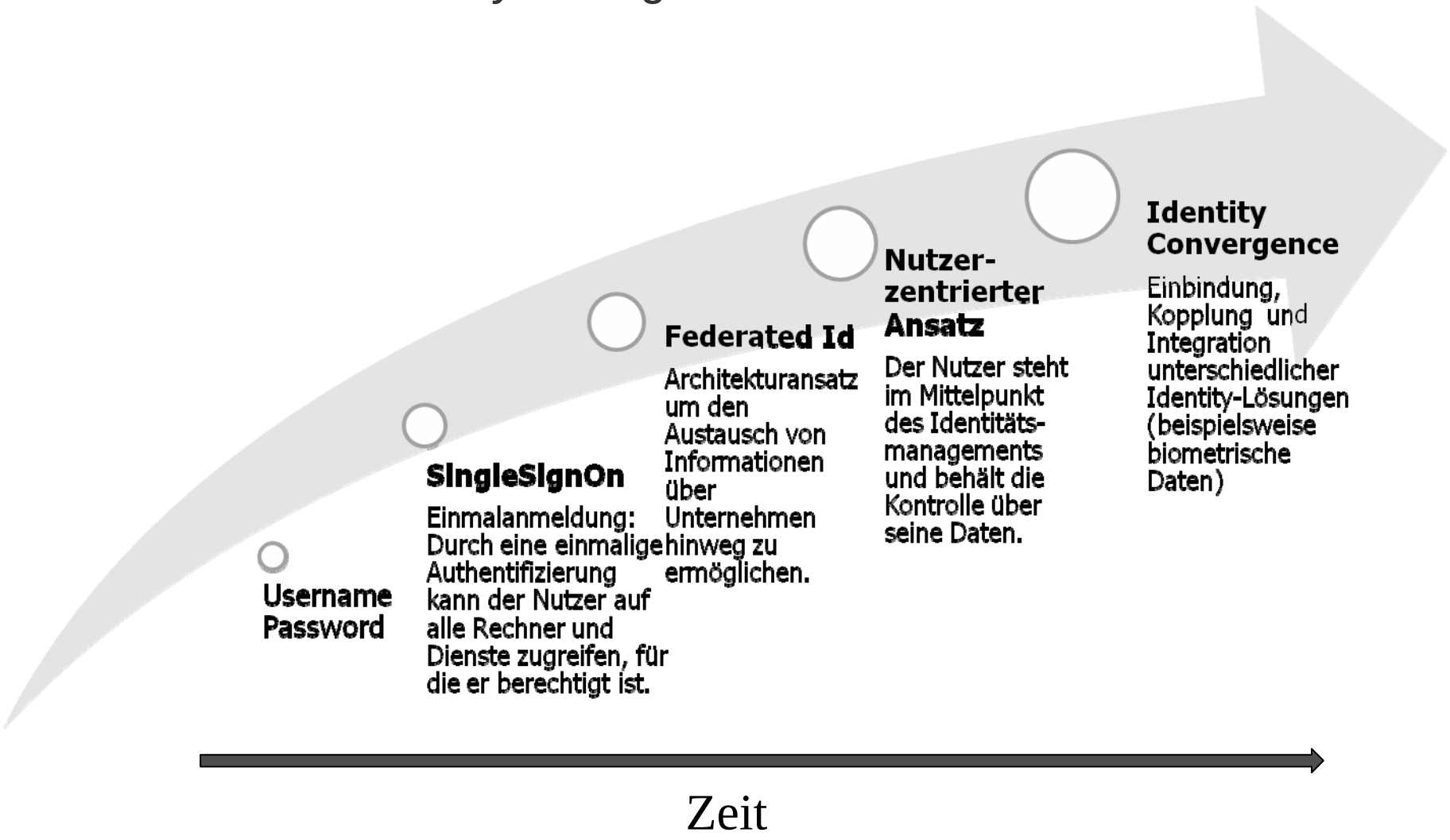
Fraunhofer FOKUS
Forschungsgruppe Elektronische Identitäten

Fraunhofer FOKUS

Evolution im Internet



Evolution von Identity Management in der IT



Jeder Mensch ist Viele!

- Viele unterschiedliche Identitäten:

Der neue Personalausweis
mit Online-Ausweisfunktion

Der neue Personalausweis
Funktionen

Zum 1. November 2010 Einführung des neuen Personalausweises.

Er vereint den herkömmlichen Sichtausweis mit drei neuen elektronischen Funktionen im Scheckkartenformat

Die neuen Funktionen
eID und QES

eID – Elektronischer Identitätsnachweis

- „Das bin ich“
- Anzeige der Identität des Dienstanbieters
- Anzeige der angefragten Daten
- Personendaten-Freigabe mit PIN
- Personendaten-Übertragung
- Beispiele: Anmeldung /Registrierung, Altersnachweis, Pseudonym

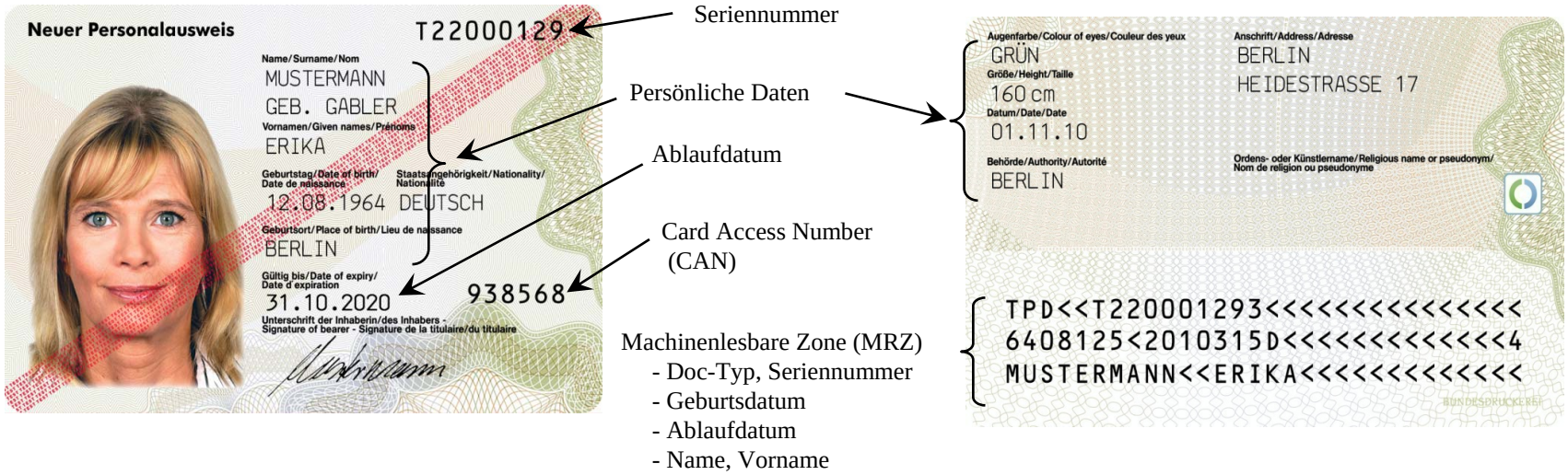
→ Gegenseitiger Identitätsnachweis

QES - Qualifizierte elektronische Signatur

- „Das habe ich unterschrieben“
- Anzeige des zu unterschreibenden Dokuments oder der E-Mail
- Signieren des Dokuments mit Signatur-PIN Eingabe
- Überprüfen der Signatur durch Empfänger
- Beispiele: Unterschreiben von Verträgen, Vollmachten, E-Mails

→ Rechtsichere elektronische Unterschrift

Physischer Ausweis



- Polycarbonatkarte in EC-Kartenformat
- Sichtausweis mit äußeren Sicherheitsmerkmalen (z.B. Hologramme, Lasergravur)
- Integrierter kontaktloser Mikroprozessor-Chip
  - Hoheitliche Anwendung (ähnlich ePass)
  - eID-Funktion und Signatur für E-Government / E-Business

Welche Daten sind im Ausweis-Chip?

Vorgeschrieben

Daten für hoheitliche Anwendungen (offline)

- Gesichtsbild
- 2 Fingerabdrücke (optional)
- MRZ-Daten (Name, Vorname, Geburtsdatum etc.)

Optional

eID-Funktion (Identitätsnachweis) für E-Government / E-Business (online)

- Name, Vorname
- Ordens-/Künstlername
- Doktorgrad
- Geburtsdatum
- Geburtsort
- Adresse
- Wohnort-ID
- Altersverifikation
- Verifikation des Wohnorts
- Pseudonym
- Sperrmerkmal

Optional

Signatur für E-Government / E-Business (online / offline)

- Signaturschlüssel
- Signaturzertifikat

für die qualifizierte elektronische Signatur nach deutschem Signaturgesetz

Innovation

Gegenseitiger Identitätsnachweis (eID-Funktion)

BürgerInnen

Ist das Unternehmen real?

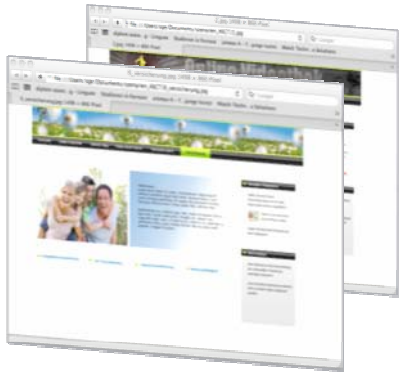
Diensteanbieter weist sich mit Berechtigungs-zertifikat aus

Sowohl Bürger als auch Diensteanbieter können sich bei Nutzung des neuen PA auf die Identität ihres Gegenübers verlassen

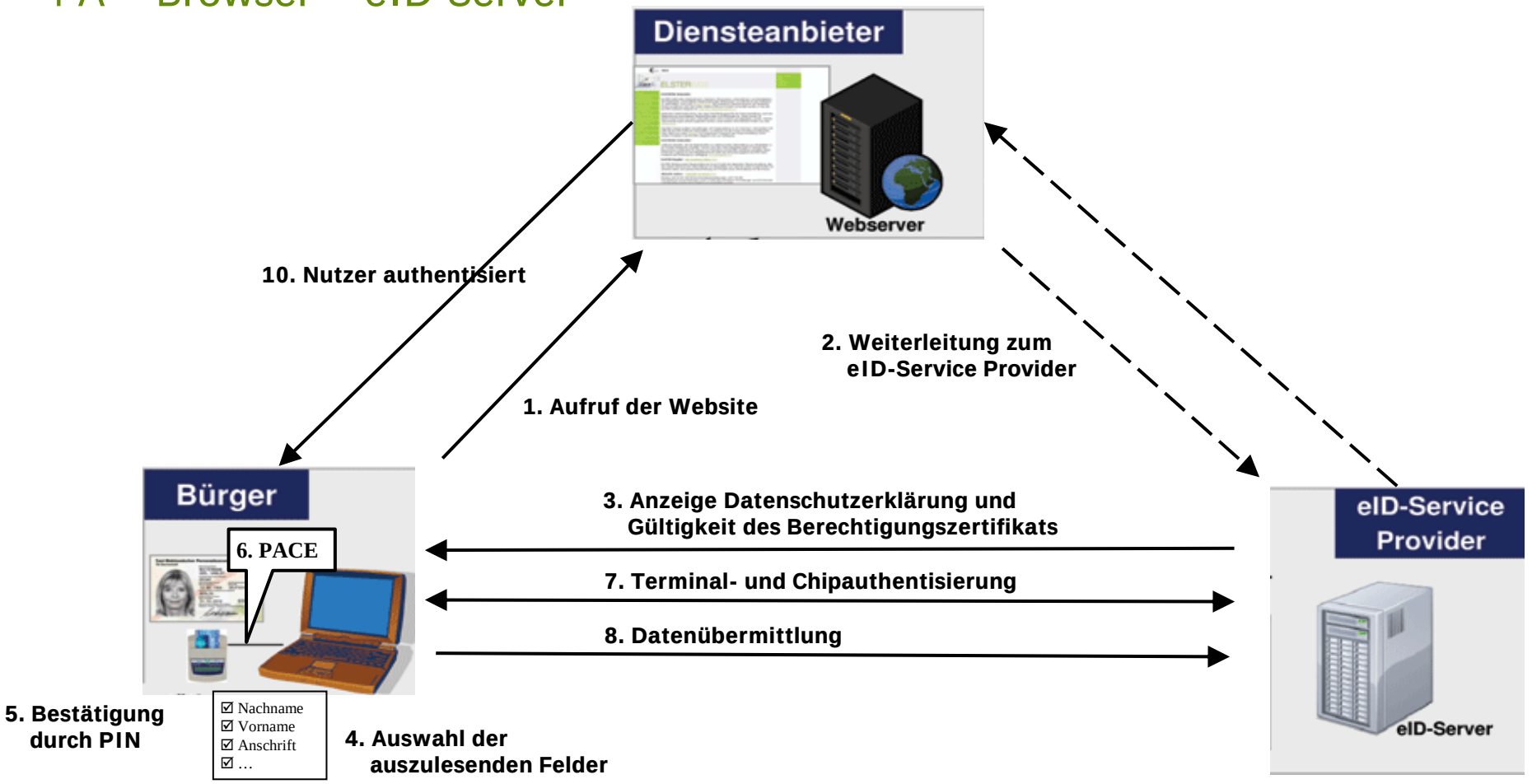
Bürger weist sich mit neuem PA aus

Diensteanbieter

Wer ist die anfragende Person?



Kommunikationsmuster
PA – Browser – eID Server



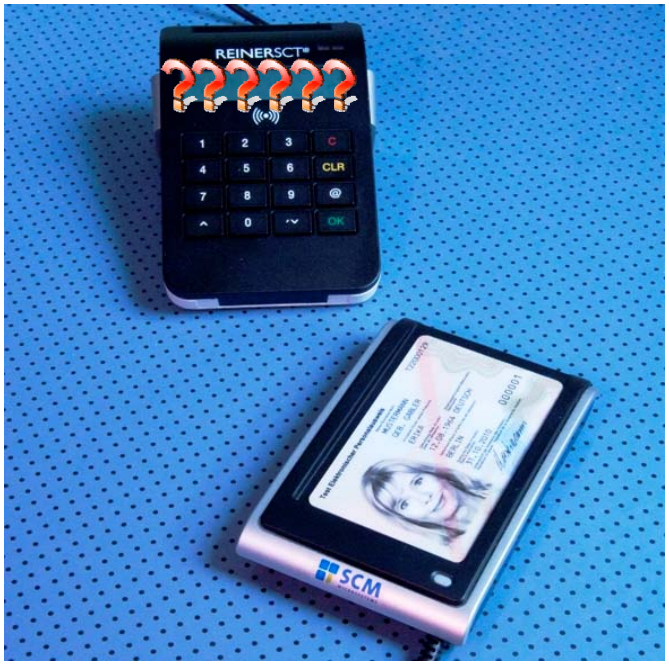
(PACE = Password Authenticated Connection Establishment)

Die neuen Funktionen
Daten

Auf dem neuen Personalausweis sind nur die Daten gespeichert, die außen sichtbar sind und nicht mehr als auf früheren Ausweisen!

PIN-Eingabe notwendig!

2 Faktor Authentisierung –
Man braucht Wissen (PIN) und Besitz (PA)



Datensparsamkeit und Datenschutz

eID – Beispiele in Europa

Wirtschaftliche Aspekte

- Bereits 8 Mitgliedsstaaten mit eIDs, weitere werden folgen
- Nationale und grenzüberschreitende elektronische Dienstleistungen
- Neue Geschäftsfelder im Internet durch sichere und vertrauenswürdige Identifikation möglich

Zeitplan bis zur Einführung

2008

2009

2010

20.11.2008
Start Registrierung zentral koord.& offener Anwendungstest

28.02.2009
Ende Registrierung für zentral koord. Anwendungstest

Ende Mai 2009
Auswahl Teilnehmer zentral koord. Anwendungstest

01.10.2009
Start zentral koord. Anwen-dungstest

01.01.2010
Start offener Anwendungstest

Ende Juli 2010
Bericht Anwendungstest

31.10.2010
Ende Anwendungstest

1. Quartal 2009
Information zur Teilnahme am Feldtest

2. Quartal 2009
Auswahl Ausweisbe-hörden Feldtest

1.Quartal 2010
Start Feldtest

2. Quartal 2010
Bericht Feldtest

01.05.2010
Start Bean-tragung von Berechtigungs-zertifikaten

01.11.2010
Einführung neuer Personalausweis

Inkrafttreten von Gesetz und Verordnungen

Der neue Personalausweis...

... wird ausführlich erprobt...

Labor- und Funktionstests	Studien/ Wissenschaftliche Untersuchungen	Anwendungs- und Feldtest
▪ Test elektronischer Identitätsnachweis ▪ Test Zusammenspiel der Hardware und Software-Komponenten ▪ Konformitätstest Spezifikation ▪ Test- und Demonstrationszentrum neuer Personalausweis	▪ Restrisiken beim Einsatz des Bürgerclients auf dem Bürger-PC ▪ Diverse White Paper zu Themen rund um den neuen Personalausweis ▪ Haftungsstudie ▪Usabilitystudie	Ab 01.10.2009 Zentral koordinierter Anwendungstest für ausgewählte Teilnehmer Ab 1.1.2010 Offener Anwendungstest für alle Interessenten Feldtest in ca. 30 Personalausweisbehörden, ab 01.10.2009

Ziele im Anwendungstest neuer Personalausweis

- Test der Infrastruktur und der erforderlichen Supportstrukturen
- Frühzeitige Einbindung der Diensteanbieter für E-Business und E-Government bei der Erprobung der Technik
- Öffentlichkeitsarbeit und Kommunikation bezüglich der Möglichkeiten der neuen Infrastruktur mit dem neuen Personalausweis
- Attraktive Anwendungsmöglichkeiten zeitnah nach der Einführung am 1. November

- Einrichtung eines Kompetenzzentrums zur Betreuung der Anwendungstests

Unterstützung durch das Bundesministerium des Innern

Teilnehmer am zentral koordinierten Anwendungstest

E-Government

Deutsche Rentenversicherung
Rathaus21 DIE E-GOVERNMENT LÖSUNG
Datenzentrale Baden-Württemberg
HSH
service-bw
T-Systems
AKDB
FRITZ&MACZIOL Software, Systeme und Dienstleistungen
Umwelt Bundes Amt DEHSt
Fraunhofer FOKUS
ITDZ BERLIN
Kroschke
]init[

E-Finanzservice

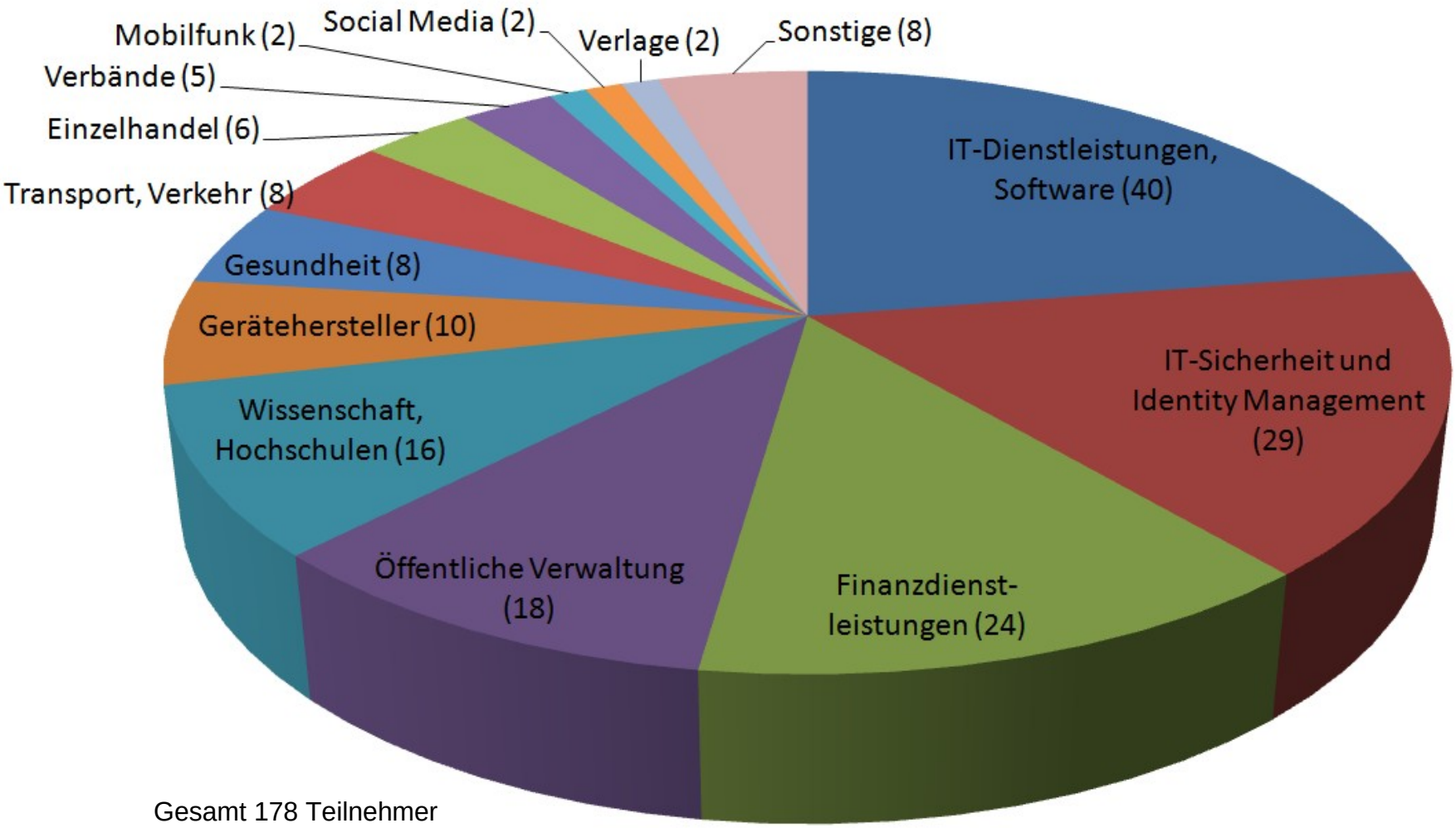
Allianz
DKB Deutsche Kreditbank AG
CosmosDirekt.
Gothaer
HUK24 DIE ONLINE-VERSICHERUNG
InterCard
LVM Versicherungen
SIZ INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH
PROVINZIAL

E-Business

FUJITSU
airberlin
WINCOR NIXDORF
VRR
WEBER
schufa
Institut für Inklusion

- Am zentral koordinierten Anwendungstest nehmen 30 Institutionen aus unterschiedlichen Geschäftsbereichen teil.

Teilnehmer am offenen Anwendungstest nach Branchen



Gesamt 178 Teilnehmer

Was wird getestet?

- Umfangreiche Tests im Vorfeld, u. a.:
  - Erprobung der Infrastruktur
  - Integration der Dienste
  - Nutzbarkeit des elektronischen Identitätsnachweises
- Im Detail werden getestet:
  - Seit Anfang Dezember 2009 der Bürgerclient und eine Test-Schnittstelle zum eID-Server
  - Seit Anfang Januar 2010 Zusammenspiel Bürgerclient und eID-Server mit Testanwendungen
  - Seit Anfang Februar testen die Dienstanbieter intensiv die Integration des zur Verfügung gestellten Java-Connectors und den zur Verfügung gestellten eID-Server in ihre eigenen Anwendungen

Unterstützung und Vorbereitung der zentral koordinierten Diensteanbieter

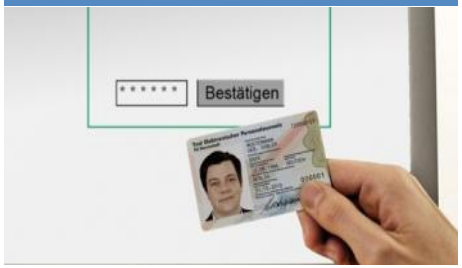
- Seit Anfang Oktober 2009: Intensive Betreuung und Begleitung der 30 zentral koordinierten Anwendungstestteilnehmer
- Oktober, November 2009: Einführungs-Workshops quer durch Deutschland (München, Darmstadt, Düsseldorf, Hannover, Berlin): Überblick über Identitätsmanagement, Architektur und Anforderungen an IT-Sicherheit
- Januar, Februar 2010: Integrationsworkshops für die Anwendungstestteilnehmer zur sicheren und effektiven Anbindung an den eID-Server

Anwendungstests im Detail

- Probanden erproben seit Februar 2010 als Musterkunden oder Mustermitarbeiter intensiv die Funktionalität
  - Es wurden bis Ende Juni mehr als 2000 personalisierte Karten ausgegeben und zahllose Mustermannfamilien
- Unterstützung bei der Beantragung der Berechtigungszertifikate und der Definition der Prozesse und Geschäftsmodelle in Kooperation mit der Vergabestelle für Berechtigungszertifikate

Aufbau und Test möglicher Anwendungen

Zugang mit Pseudonym

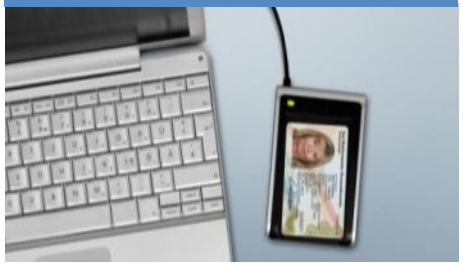


Altersverifikation

Bürgerdienste

Kiosksysteme / Infoterminals

Automat. Formularbefüllung



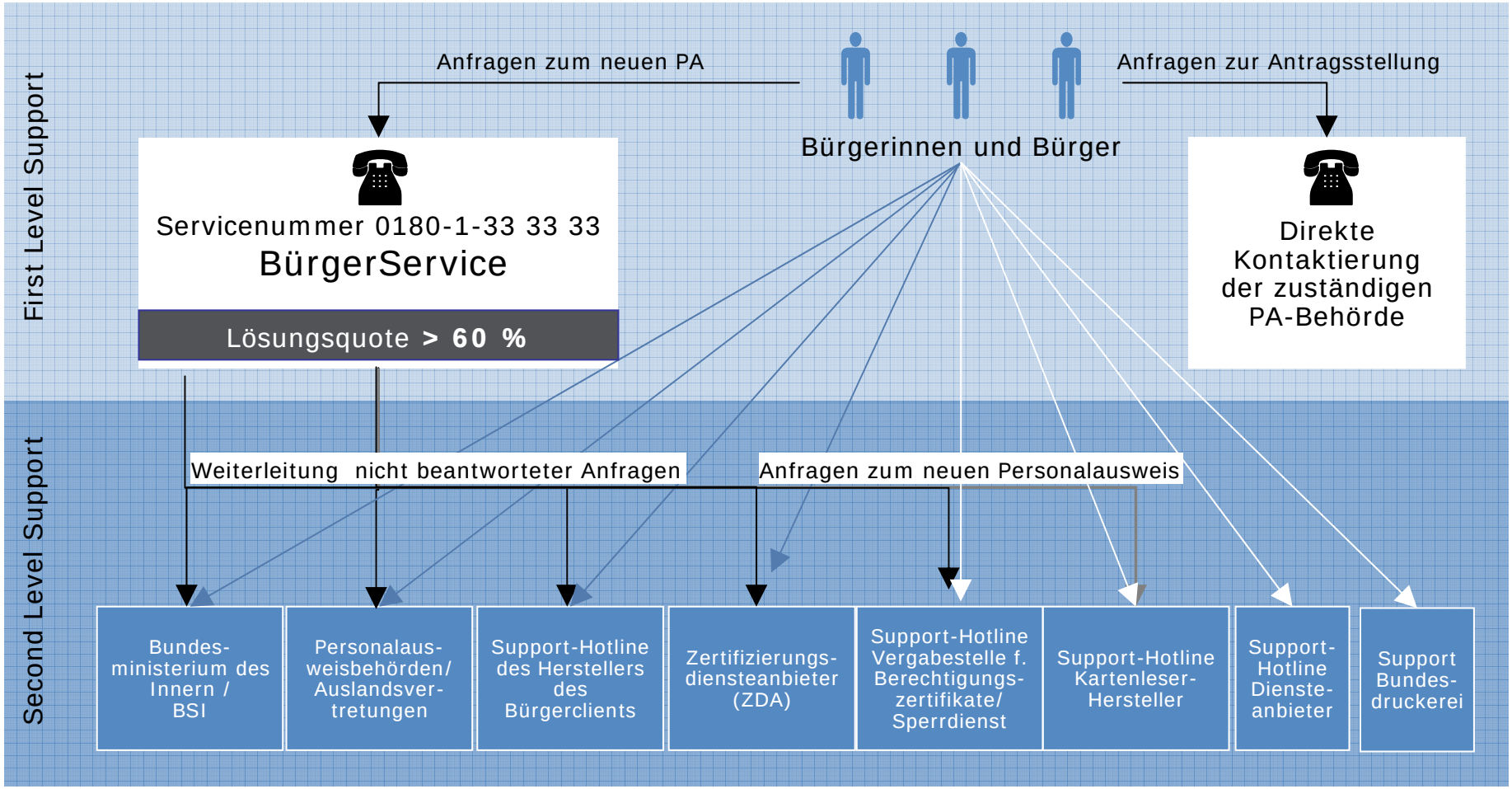
Elektronische Signatur

Online-Registrierung

Zutrittskontrollen

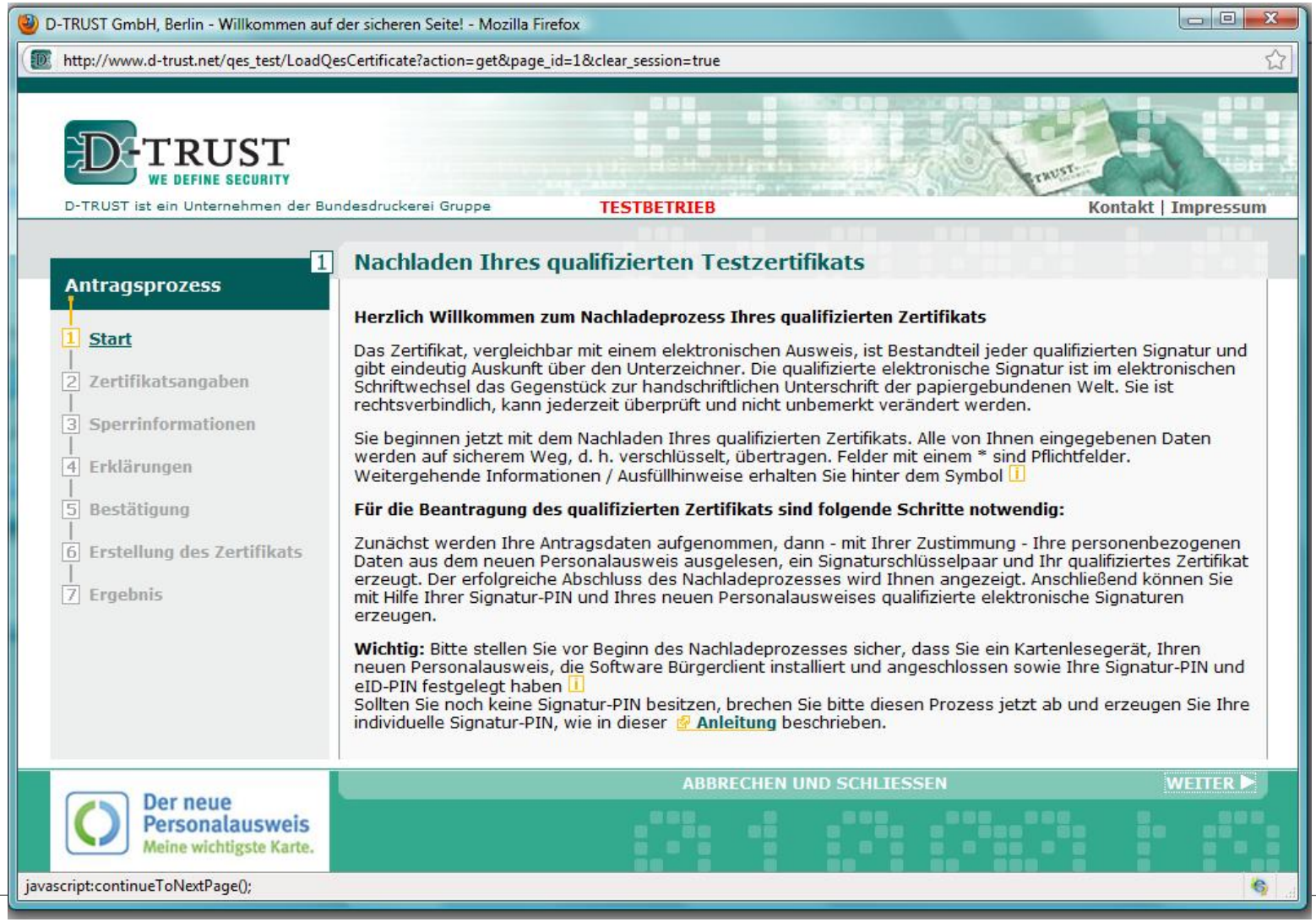
Barrierefreie Internetdienste

Unterstützung des Bürgerservicezentrums/Bürgerhotline

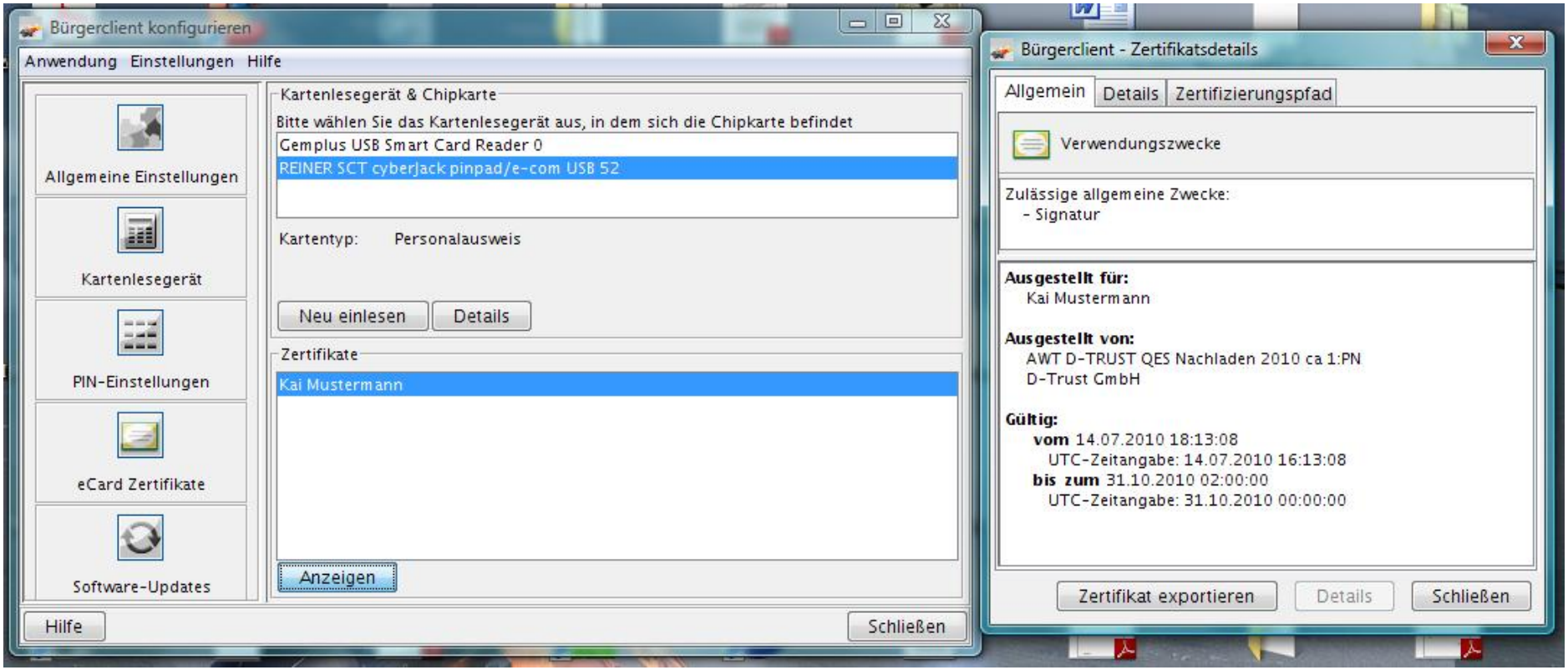


Standardverfahren: Über BürgerService
Nicht-Standardverfahren: Über BürgerService
Standardverfahren: Direkt an Second Level Support
Nicht-Standardverfahren: Direkt an Second Level Support

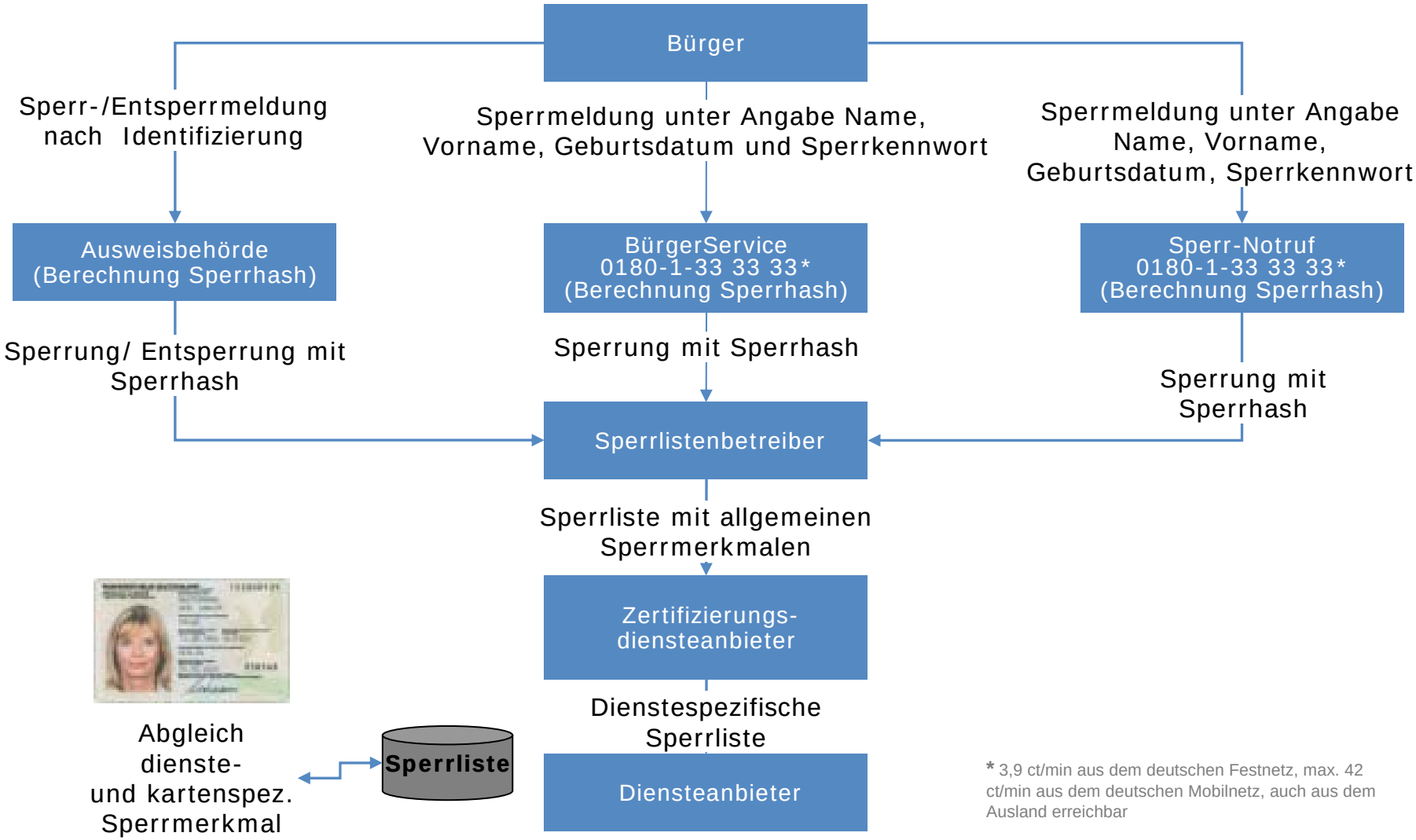
Aktueller Test: QES nachladen



Aktueller Test: QES anwenden



Ongoing: Test der Sperrprozesse/ Sperrmöglichkeiten



* 3,9 ct/min aus dem deutschen Festnetz, max. 42 ct/min aus dem deutschen Mobilnetz, auch aus dem Ausland erreichbar

Unser Beitrag: Test- und Demonstrationszentrum
im Fraunhofer FOKUS

- Aufbau und Angebot eines „zentralen Anlaufpunktes und InfoPoint rund um den neuen Personalausweis“
- eIdentity-Lounge und Secure eIdentity-Labor
- zahlreiche Anwendungen mit dem neuen Personalausweis (plattformunabhängig, OpenSource, Automaten, mobile Geräte und vieles mehr)
- Evaluierung und Analyse von zukünftigen Produkten für den neuen Personalausweis

Bundesministerium des Innern

Resumee

- **Viele Baustellen geschlossen und erfolgreiche Einführung zum 1.11. möglich!**
- Aufwände für die Integration des eID-Server in eigene Infrastrukturen überschaubar.
- Sichere und vertrauenswürdige Identitfikation mit der Infrastruktur des neuen Personalausweises möglich.
- Die AusweisApp als kostenfreie und quelloffene Software ist hierbei eine gute Grundlage!

Resumee/ Herausforderungen

- Verfügbarkeit des eID-Server sehr wichtig
- Usability insgesamt (Download und Installation Software, Kartenleser, unterschiedliche OS, Email-Clients, Browser, Eingabe der CAN)
- Genaue Definition der Prozesse für den Antrag bei der Vergabestelle für Berechtigungszertifikate notwendig
- Unterschied zwischen QES und Online-Ausweisfunktion
- Ausrollen von Basiskartenlesern (Basis vs. Komfort) -> IT-Sicherheitskit
- Weitere Softwarelösungen notwendig (mobile Lösungen, Offline-Anwendungen)

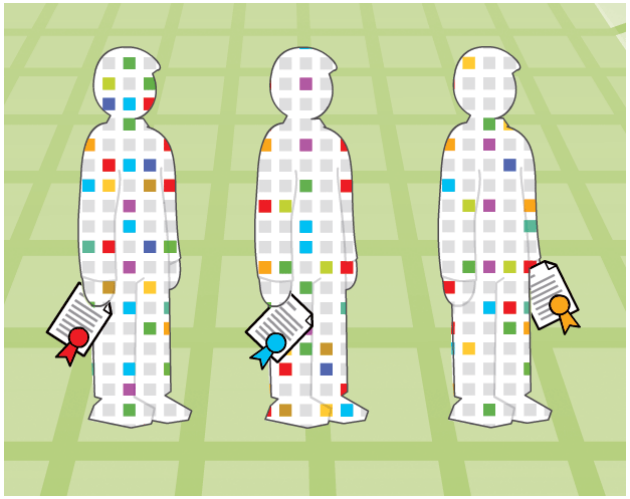
Resumee/ Herausforderungen

- Gesetzliche Anpassung notwendig um in vielen Prozessen eID-Funktion nutzen zu können
- Weitere Kommunikation/ Aufklärung Richtung neuer Personalausweis notwendig (insbesondere Online-Ausweisfunktion, da optional) Aufklärungskampagne für Bürger
- Schulung der Personalausweisbehörden
- Harmonisierung der nationalen Ansätze mittelfristig notwendig

Auf dem Weg zu einer neuen sicheren Internetwelt mit dem neuen elektronischen Personalausweis

- Moderne Industrienationen benötigen eine innovative und sichere Infrastruktur zum Management von elektronischen Identitäten.
- Neue sichere Geschäftsmodelle und neue Dienste (Impulse auch für neue Produkte der IT-Wirtschaft) benötigen zukünftig ein vertrauenswürdiges hoheitliches Dokument.
- Vertrauen im digitalen Umfeld muss durch Privatheit, Datenschutz sowie vertrauenswürdige Identitäten gestärkt werden.

Der neue Personalausweis ist ein wichtiger Schritt um eine sichere Welt im Internet voranzutreiben.



Jens Fromm

Fraunhofer FOKUS
Forschungsgruppe eIdentitäten
Kaiserin-Augusta-Allee 31, 10589 Berlin,
Deutschland

Tel + 49 30 3463 7115
Fax + 49 30 3463 8000

Internet: www.fokus.fraunhofer.de
Email: jens.fromm@fokus.fraunhofer.de