

# Identitätsmanagement der nächsten Generation

...mit der österreichischen Handy-Signatur

Dr. Arne Tauber  
Wien, 20.10.2014



**EGIZ**

E-Government Innovationszentrum

Das E-Government Innovationszentrum ist  
eine gemeinsame Einrichtung des  
Bundeskanzleramtes und der TU Graz



BUNDESKANZLERAMT  ÖSTERREICH

# Eindeutige Identität

## THEATRE NEWS

### What's in a name?

10:55am Thursday 25th February 2010

Print Email Share

IDENTITY theft is no joke – the government puts the cost of this particular type of fraud at between £1.5 and £1.7 billion a year.

And yet comedian Bennett Arron, himself a victim of stolen identity, manages to see the funny side in his new show *It Wasn't Me, It Was Bennett Arron*. In the show he recounts the series of bizarre experiences that over the course of a decade, left him homeless, penniless and resulted in a jail sentence.

"The last thing I expected was to do a comedy show about it," explains Bennett, "I was about to buy my first home in north London when I received a letter from the bank saying they'd discovered I had huge debts and couldn't go



Bennett Arron

**KLEINE ZEITUNG**

Zuletzt aktualisiert: 20.02.2010 um 05:48 Uhr [\(2 Kommentare\)](#)

## Ein Datenzwilling wider Willen

Sein virtueller Datenzwilling kostete Thomas Huber reale Nerven.

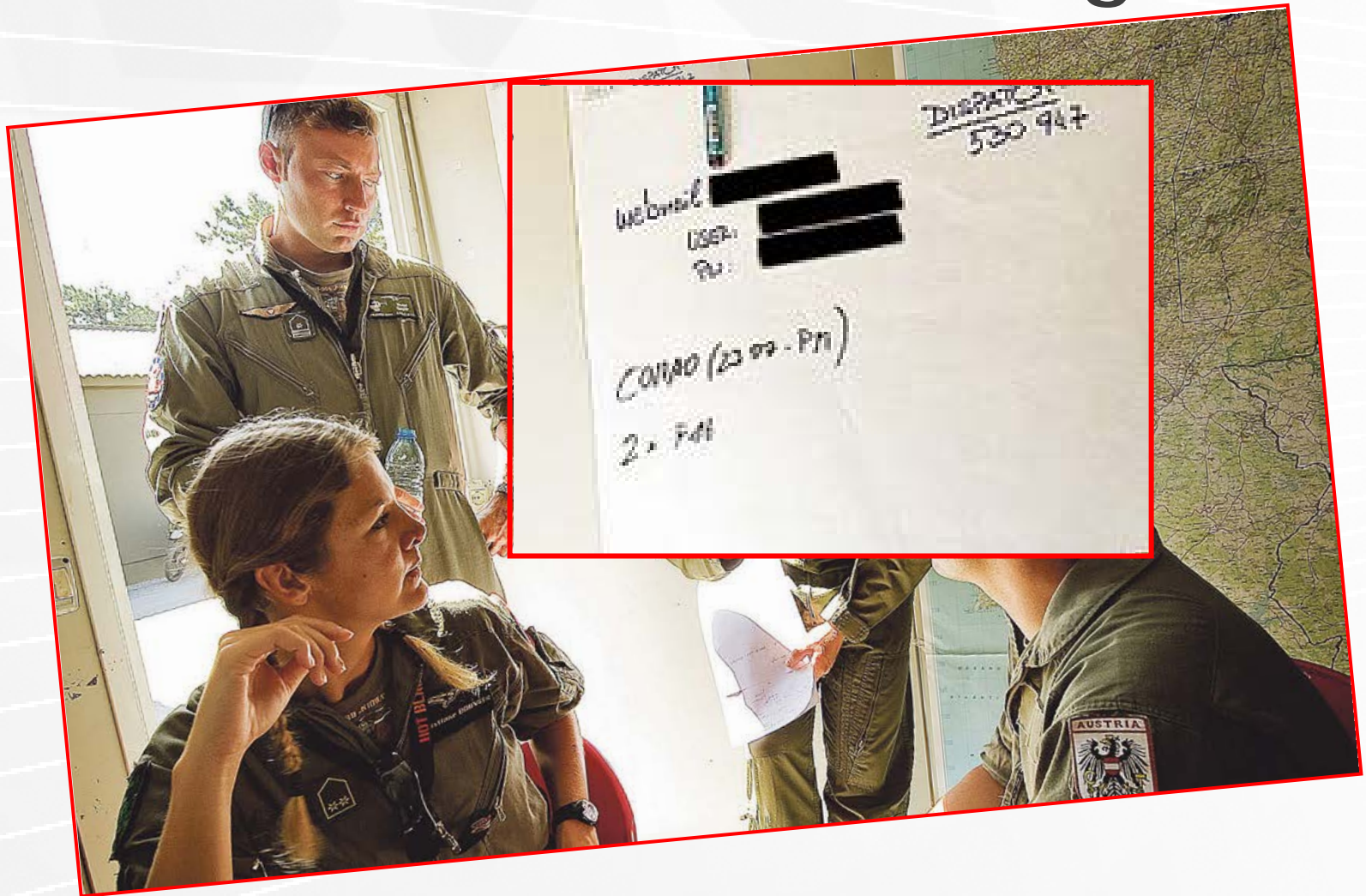


Thomas Huber hatte einen Datenzwilling

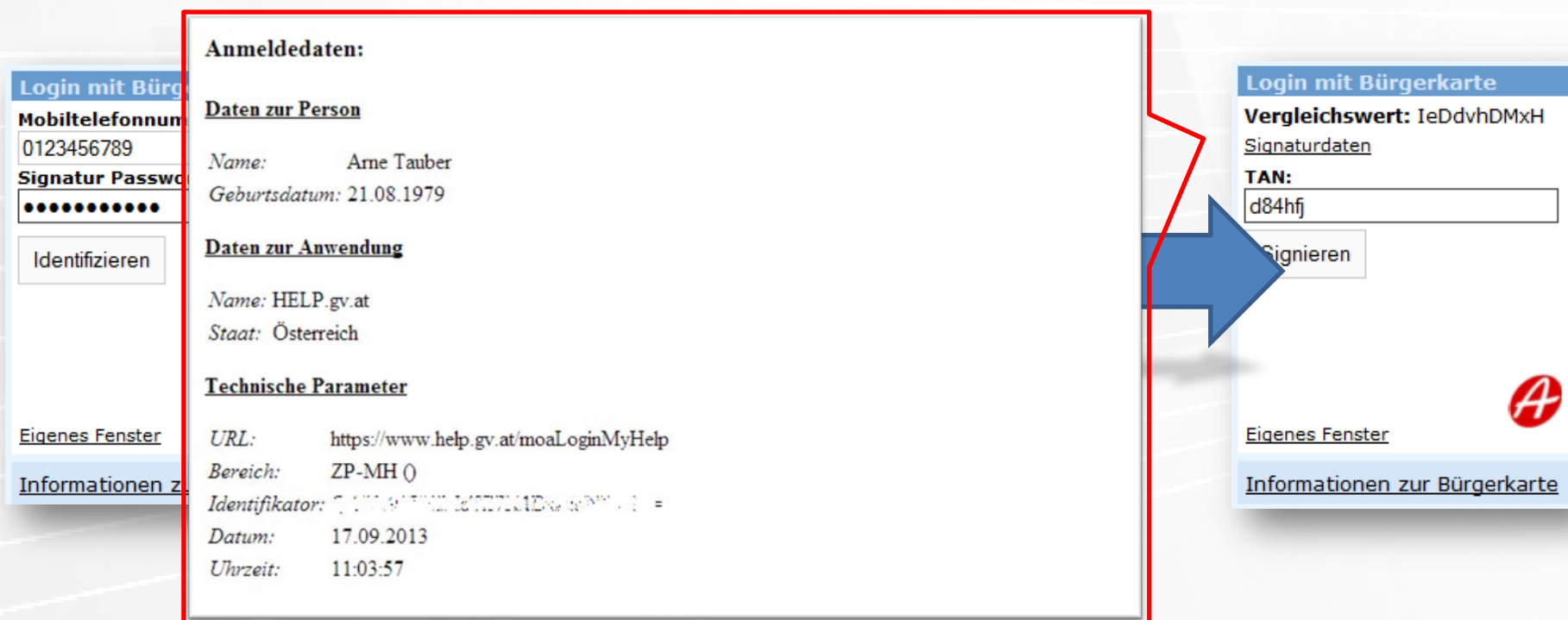
nd persönliche Daten – in Zeiten von Facebook und Google eine heikle  
Datenschützer warnen vor Datenmissbrauch – ein Aufschrei, der spätestens dann  
harmlos erscheint, wenn man selbst um die eigene Identität kämpfen muss. Nie  
mal.

h vor einigen Jahren davon erfahren, einen Datenzwilling in Tirol zu haben.  
parprämie brachte den Stein ins Rollen. Vorname, Nachname,  
Jahr – alles ident. Sogar die Sozialversicherungsnummer war dieselbe.  
Kampf gegen die österreichische Bürokratie seinen Lauf. Ob Steuer-  
kamnte in seine Daten einsehen, er in meine – laut Gesetz eigentlich ein  
Geheimhaltungsanspruch. Erstmals wurde ich hautnah mit dem Mythos des  
und zwei Jahre lang mussten mein Vater und ich intervenieren. Sozialversicherung und  
Finanzamt wirkten ratlos, zu komplex schienen die Verstrickungen mit meinem Datenzwilling zu  
sein. Blieb auf Anraten meines Anwaltes nur mehr der Gang in die Öffentlichkeit. Erst durch

# Starke Authentifizierung



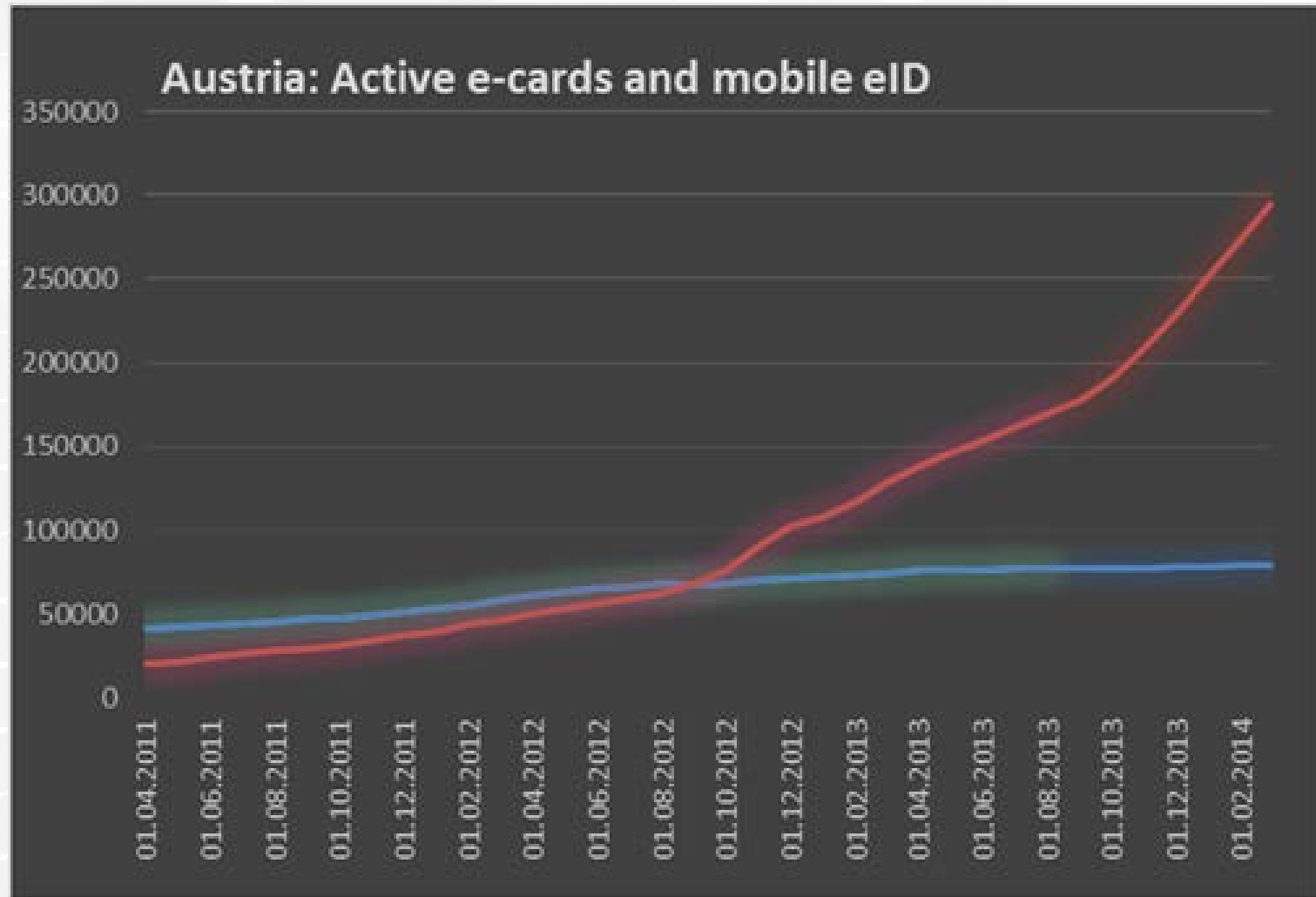
# Einfache Bedienung



# EU E-Government Benchmark 2014 (Good Practices)

- » *“It is an easy-to-use qualified electronic signature that fosters trust and security, reliability and authenticity for Government and beyond.”*
- » *“Austria literally achieved in squaring the circle: with this innovative solution a qualified electronic signature can be created in the easiest possible way by simply using a standard mobile phone. Barriers from the need of soft- or hardware installation and additional investments completely fall away.”*

# Erfolgsmodell Handy-Signatur



# MOA-ID 1.x – State of the art?

- » Bürgerseite
  - » Aktuellste SL-Spezifikation
  - » Sämtliche BKUs
- » Identity/Service Provider
  - » Identitätsprotokolle
    - » SAML 1.0 (2002)
      - » Artifact Resolution
  - » Weitere IdP-Features?



Seite: <http://evateuling.blogspot.co.at>

# MOA-ID 1.x – State of the art?

- » Bürgerseite
  - » Aktuellste SL-Spezifikation
  - » Sämtliche BKUs
- » Identity/Service Provider
  - » Identitätsvermittlung
    - » SAML 1.0 (2002)
    - » Artifact Resolution
  - » Weitere IdP-Features?

**Isolierter Betrieb**



Seite: <http://evateuling.blogspot.co.at>



# Identitätsmanagement

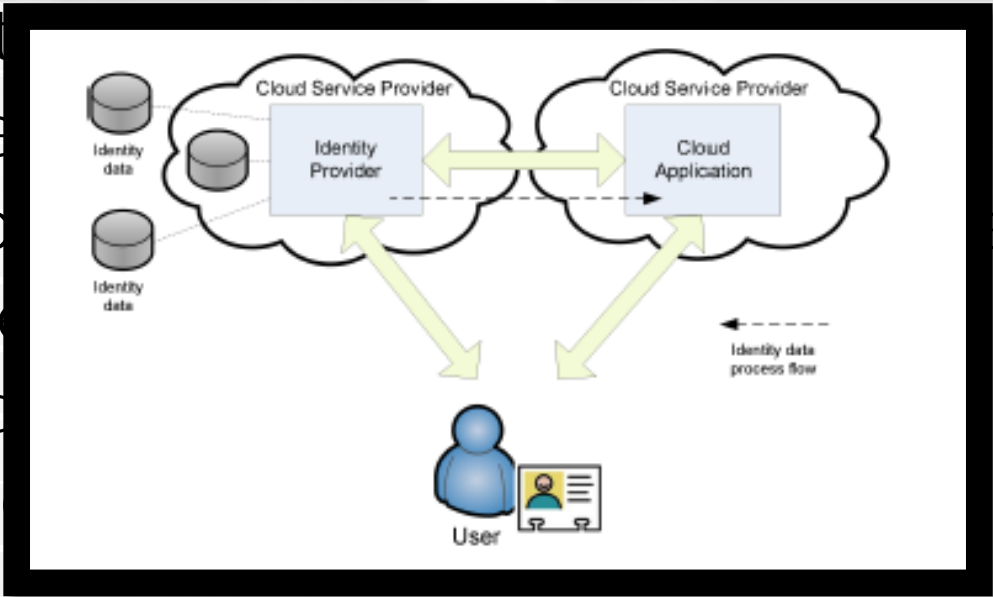
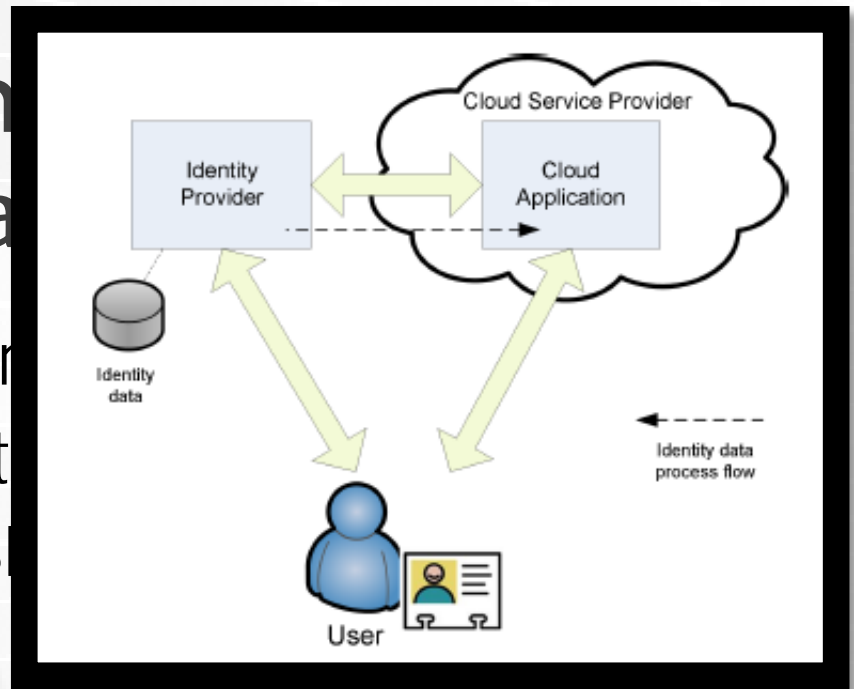
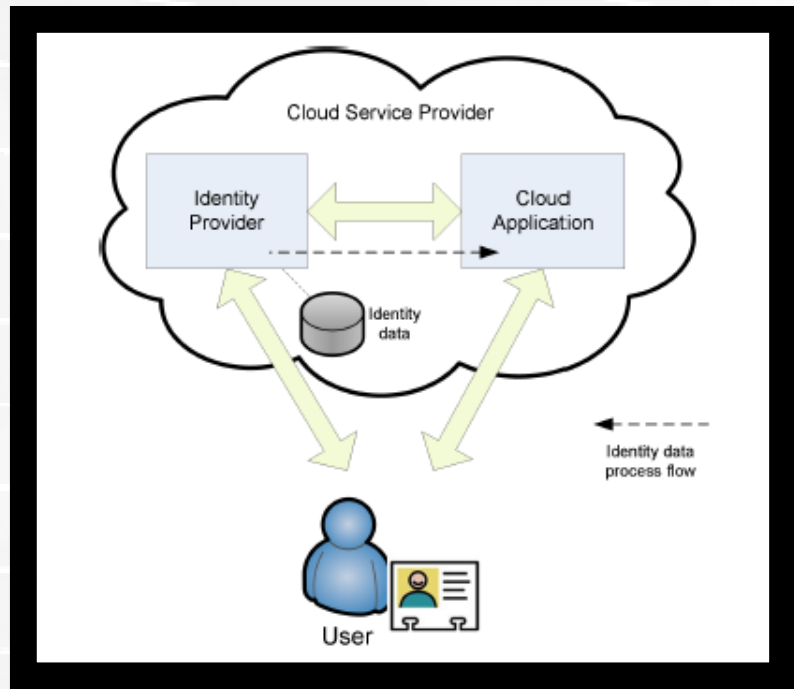
## Aktuelle Trends

- » Mobile Computing
  - » MDM, BYOD, ...
- » Cloud Computing
  - » IaaS, PaaS, SaaS, XaaS, ...
  - » Public, Private, Community, Hybrid cloud
- » Interoperabilität
  - » Federation, Broker, Bridges, ...

# Identity Management as a Service (IDMaaS)

- » Handy-Signatur eine Art „Cloud Service“?
- » Ziele eines „zentralisierten“ Betriebs
  - » Hochverfügbarkeit / Skalierbarkeit
  - » Kostenreduktion
  - » Multi-tenancy (Mandatenfähigkeit)
- » Modelle
  - » Public Cloud (Datenschutzbedenken)
  - » Private Cloud
  - » Hybrid Cloud (Enterprise & Cloud)
  - » Shared Service





em  
Ma  
e Ar  
sient  
t / S

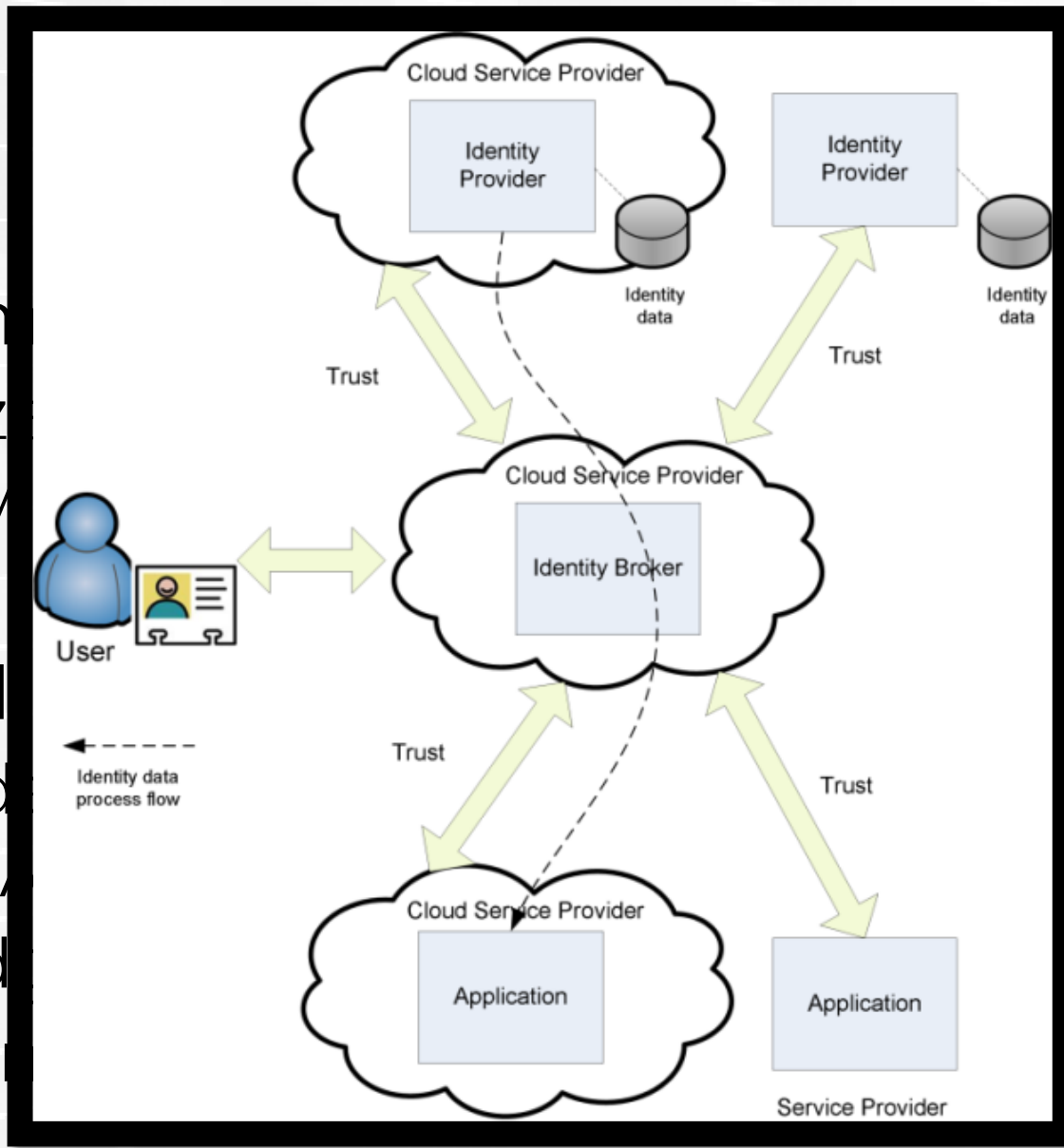
- » Multi-tenancy
- » Modelle
- » Public
- » Private
- » Hybrid
- » Share

en)

# Interoperabilität

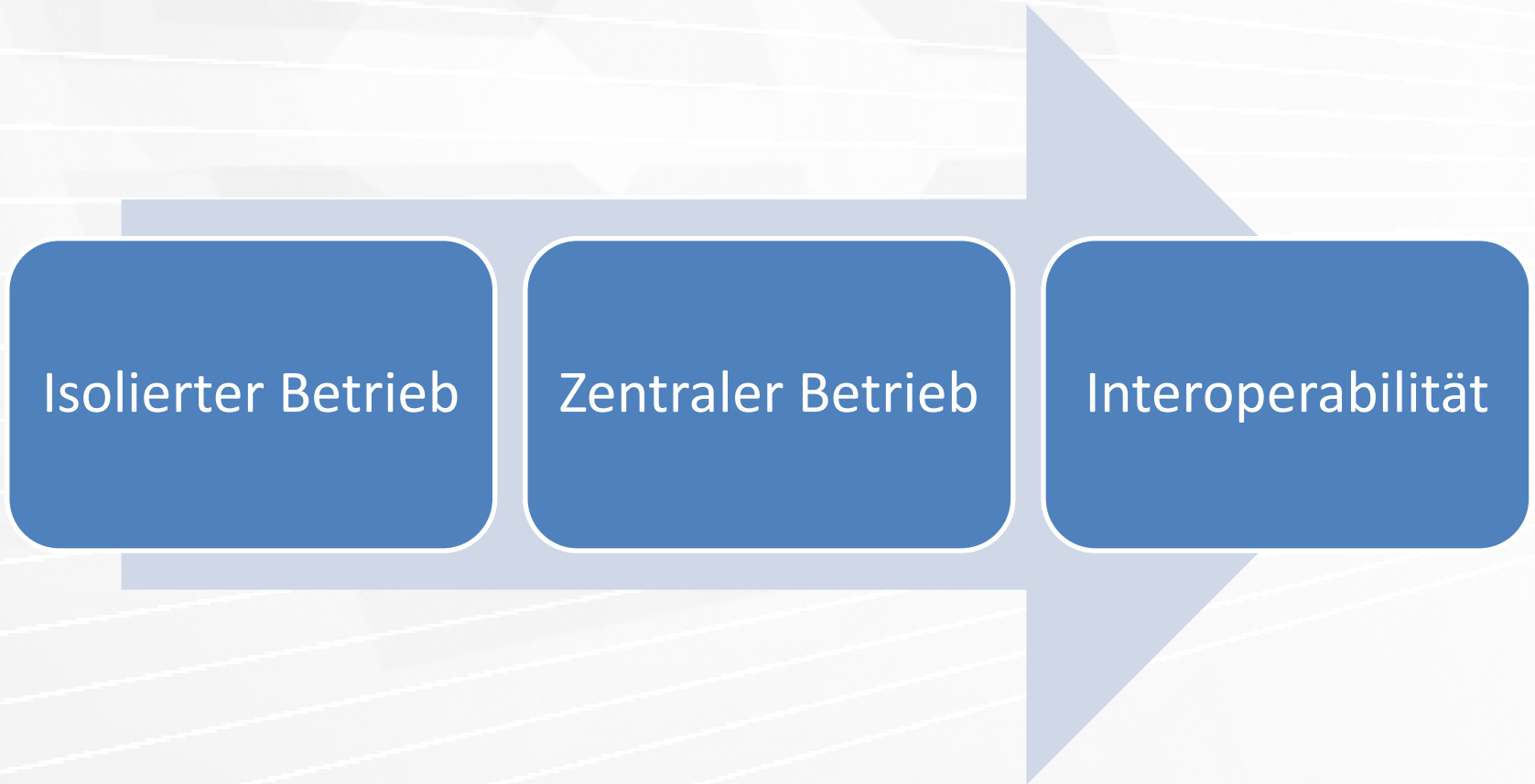
- » Fragmentierte IDM Landschaft
  - » Unzählige Produkte, Systeme, Plattformen
    - » Microsoft, IBM, Oracle, ...
- » Trend geht in Richtung Interoperabilität
  - » Federation / Standards
    - » SAML 2, OAuth, OpenID, CAS, WS-Federation
  - » Bridges
  - » Identity Broker (Skidentity)

- » Fragmentation
- » Unz...
- » M...
- » Trend...
- » Fed...
- » S...
- » Brid...
- » Ide...



formen  
 ilität  
 eration

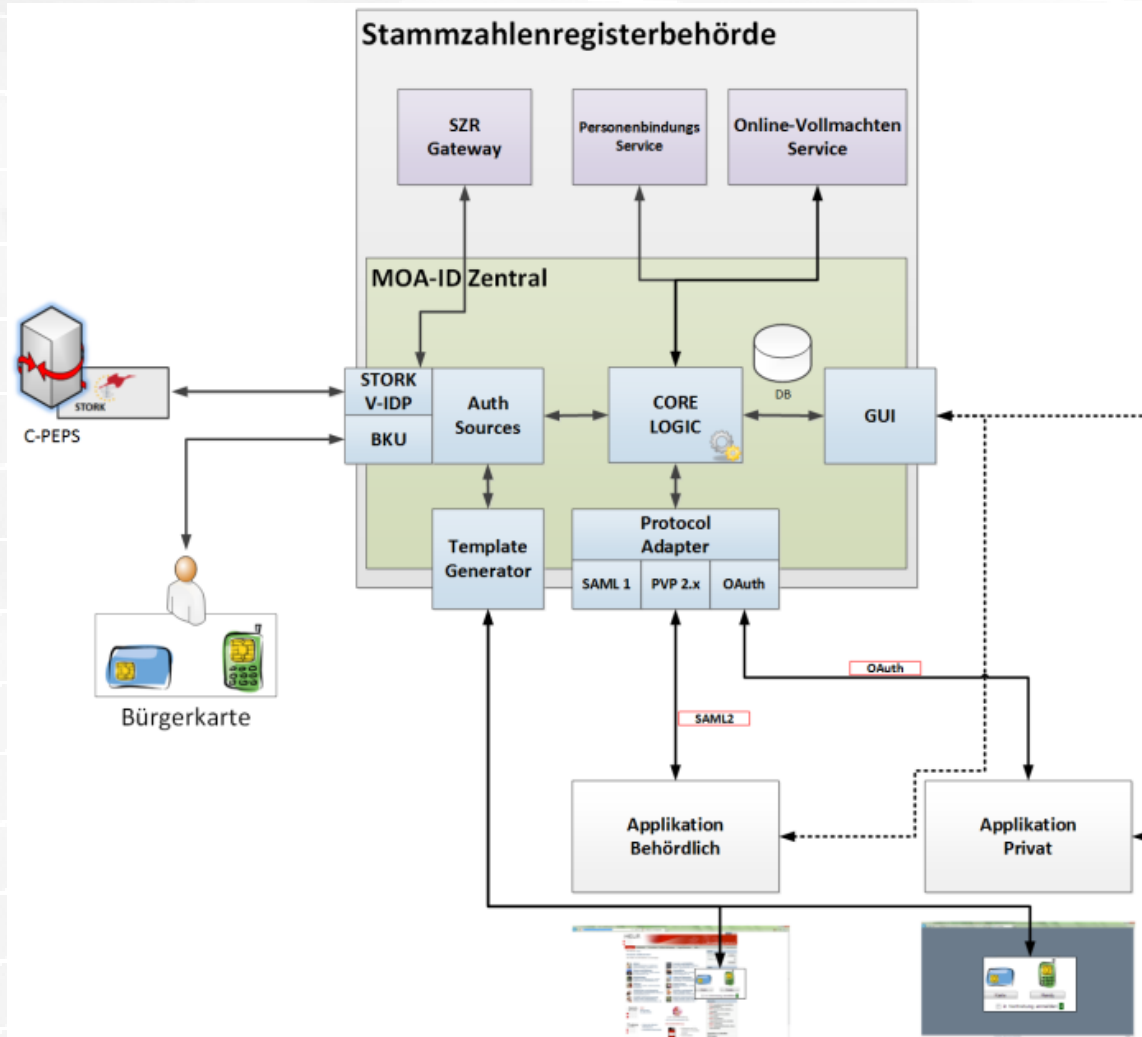
# Paradigmenwechsel



# Modulares Identitätsmanagement

- » Trennung von Programmlogik & Daten
  - » Persistente Daten (Konfiguration)
  - » Flüchtige Daten (Session Informationen)
- » Identitätsprotokolle
  - » SAML1, SAML2 (PVP2), STORK, OAuth, ...
- » Authentifizierungsmechanismen
  - » Handy-Signatur / STORK / Next?

# MOA-ID 2.x Architektur





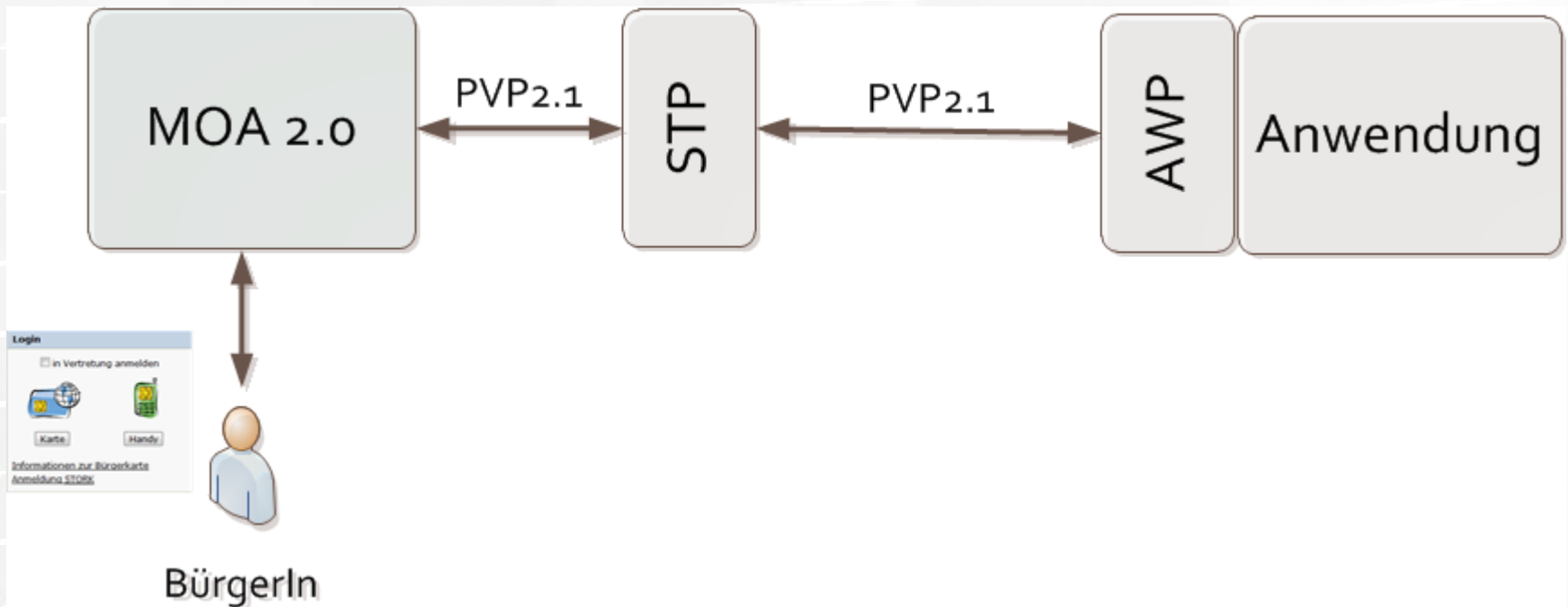
# Features (1)

- » Clusterfähigkeit / Skalierbarkeit
  - » 1 Datenbank – n MOA Instanzen
- » Multi-tenancy
  - » DB-basierte Konfiguration
  - » GUI-basierte Registrierung / Verwaltung
- » Plugin-basierte Identitätsprotokolle
  - » PVP2 (Verwaltung) als Standardvariante
  - » OAuth für Privatwirtschaft
  - » STORK (ausl. Identitäten)
  - » SAML1 (Abwärtskompatibilität)

# SAML 2 (PVP2 Profil)

» PVP 2.1

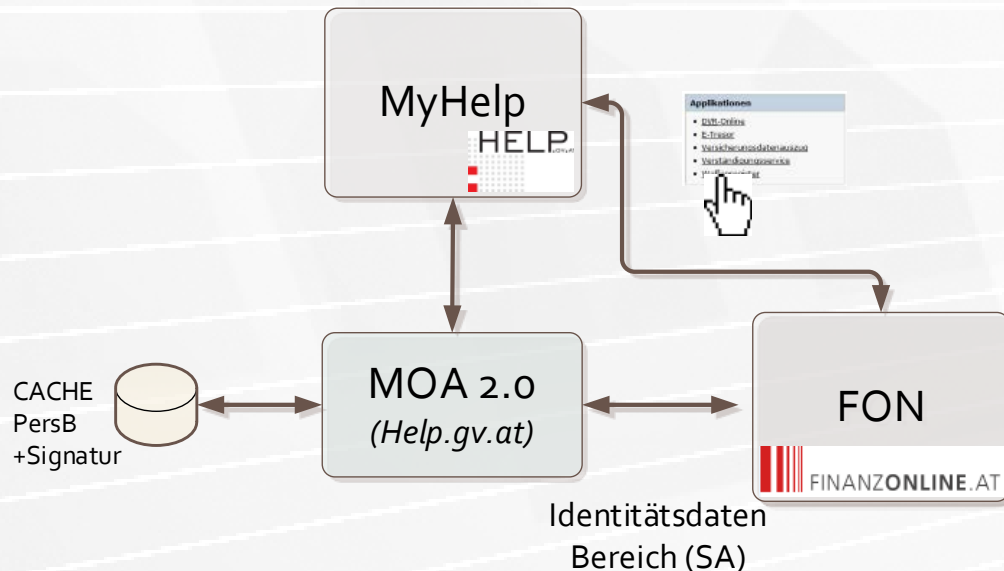
» E-Government Attribut Profil



# Features (2)

- » Single-Sign-On (SSO)
  - » 1x Authentifizieren, n-mal Anmelden
- » Federated SSO
  - » Weitergabe von Anmeldedaten zwischen MOA Instanzen
- » Single-Logout (SLO)
- » Statistikfunktion (DB)
- » Integrierte Monitoringfunktionalität
- » Fehlerhandling, Templategenerierung, ...

# SSO von MyHelp zu FinanzOnline (Gleiche Domäne)



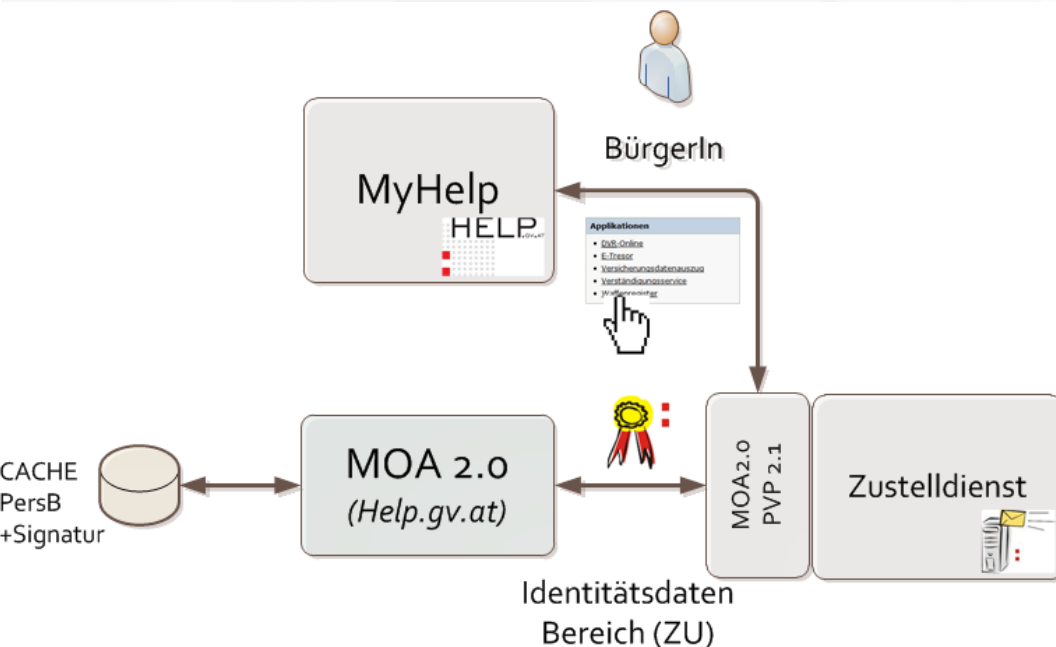
- » Link Klick „FON“
- » Redirect zu FON
- » FON holt Identitätsdaten von MOA 2.0 (BRZ) ab über
  - » Assertion von MOA berechnet
- » Voraussetzungen:
  - » MOA 2.0

# Features (2)

- » Single-Sign-On (SSO)
  - » 1x Authentifizieren, n-mal Anmelden
- » Federated SSO
  - » Weitergabe von Anmeldedaten zwischen MOA Instanzen
- » Single-Logout (SLO)
- » Statistikfunktion (DB)
- » Integrierte Monitoringfunktionalität
- » Fehlerhandling, Templategenerierung, ...

# SSO von MyHelp zu Zustelldienst (Unterschiedliche Domänen)

- » Link Klick „ZD-X“
- » Redirect zu MOA (2.0) des ZD
- » MOA 2.0 (ZD) holt Identitätsdaten von MOA 2.0 (Help) ab über
  - » PVP 2.1 (C2GToken)
  - » Berechnung bPK aus PersB Cache
- » Voraussetzungen:
  - » MOA 2.0 / PVP 2.1
- » Anmerkung: Abholung von Zustellstücken über PVP2.1 Signatur = automatisiert ausgelöste Signatur nach §35(3) ZustG



# Features (2)

- » Single-Sign-On (SSO)
  - » 1x Authentifizieren, n-mal Anmelden
- » Federated SSO
  - » Weitergabe von Anmeldedaten zwischen MOA Instanzen
- » Single-Logout (SLO)
- » Statistikfunktion (DB)
- » Integrierte Monitoringfunktionalität
- » Fehlerhandling, Templategenerierung, ...

# Automatische Templategenerierung

HELP.gv.at Deutsch | English


Amtswege leicht gemacht


[Home] Behörden Formulare / Online-Amtswege Begriffslexikon Hilfe Über HELP.gv.at


Sie sind hier: [Home](#)


## Herzlich willkommen!


Hier finden Sie Informationen zu Amtswegen.

 **Arbeit**  
[Ältere Arbeitnehmer](#), [Arbeitsuche](#), [Bewerbungstipps](#), [Kündigung](#), etc.


 **Bauen und Wohnen**  
[Wohnen](#), [Grundbuch](#), [Umzug](#), [Bauen](#), [Grundstückskauf](#), etc.


 **Behinderung**  
[Kindheit](#), [Kfz \(Behinderung\)](#), [Pension \(Behinderung\)](#), [Rehabilitation](#), etc.


 **Bildung**  
[Universität](#), [Schule](#), [Fachhochschulen](#), [Ferialpraxis](#)


 **Dokumente und Ausweise**  
[Führerschein](#), [Personalausweis](#), [Reisepass](#), [Namensänderung](#), etc.


 **Familie und Partnerschaft**  
[Geburt](#), [Heirat](#), [Alleinerziehung](#), [Scheidung](#), [Lebensgemeinschaften](#), etc.


 **Freizeit und Mobilität**  
[Kfz](#), [Vereine](#), [Rad fahren](#), [Haustiere](#), [Reisen](#), [Veranstaltungen](#), etc.

 **Jugendliche**  
[Jugendrechte](#), [Lehre](#), [Berufswahl](#), [Chancengleichheit](#), etc.

 **Leben in Österreich**  
[Aufenthalt](#), [Staatsbürgerschaft](#), [Strafreister](#), [An-/Abmeldung](#), etc.

 **Senior/innen**  
[Beihilfen für Senioren](#), [Sicherheit für Senioren](#), etc.

 **Soziales und Notfälle**  
[Katastrophenfälle](#), [Pflege](#), [Todesfall](#), [Armut](#), [Sachwalterschaft](#), etc.

 **Steuern und Finanzen**  
[Pension](#), [Pendler](#), [Erbten](#), [Beihilfen](#), [Arbeitnehmerveranlagung](#), etc.



**Suche**

Suchbegriff



Themen von A bis Z ...

**Login**

in Vertretung anmelden

[Informationen zur Bürgerkarte](#)  
[Anmeldung STORK](#)

 Follow us on [Twitter](#)  Find us on [Facebook](#)

**Aktuelles**

- **Aktuell!** [Thema des Monats Juni: Reisen](#)
- **NEU!** [KULTUR: Add](#)

**AKTUELL: [Hochwasser-Hilfe](#)** **Unbedingt JETZT: [Studienbeginn Herbst 2013](#)**



# Ausblick

- » Neue Technologien
  - » SMS Alternativen, ...
- » Modularisierung Attribute Provider
  - » Derzeit Online-Vollmachten
  - » Weitere Registerabfragen (ZMR, ...)
- » Betrieb als kritische Infrastruktur

**Vielen Dank für die  
Aufmerksamkeit!**

Arne Tauber – [Arne.Tauber@egiz.gv.at](mailto:Arne.Tauber@egiz.gv.at)  
[www.egiz.gv.at](http://www.egiz.gv.at)



**EGIZ**

E-Government Innovationszentrum