

---

# Identität und Datenschutz Ein Widerspruch?

Tagung: E-Government konkret  
18. 11. 2005, Basel

**[Arno.Hollosi@cio.gv.at](mailto:Arno.Hollosi@cio.gv.at)**

# Motivation

- E-Government muss ...
  - vertrauenswürdig sein
  - sicher sein
  - effizient sein
  
- ... deshalb benötigt man ...
  - Eindeutige Identifikation
  - Datenschutz
  - Signatur
  - Verschlüsselung

# Umsetzung

- 12 Ministerien, 9 Länder, 2348 Gemeinden
  
- Informelle Gremien
  - IKT-Bund, IKT-Bund-Länder
  - Plattform Digitales Österreich
  
- Bereich IKT-Strategie im BKA
  - Begleitet, entwickelt, spezifiziert
  - Eigenes Budget

# Rechtliche Grundlage

- E-Government Gesetz
  - in Kraft seit März 2004
  - Verordnungen
    - Verwaltungssignaturverordnung
    - Bereichsabgrenzungsverordnung
    - Stammzahlenregisterverordnung
    - Ergänzungsregisterverordnung
  
- Signaturgesetz und Signaturverordnung
  - (qualifiziertes) Zertifikat
  - Zertifizierungsdiensteanbieter (ZDA)

# Stammzahl

- **Eindeutige Identität (§2 Z2):**  
*die Bezeichnung der Nämlichkeit eines Betroffenen durch ein oder mehrere Merkmale, wodurch die unverwechselbare Unterscheidung von allen anderen bewirkt wird*
  
- **Stammzahl (§2 Z8):**  
*eine zur Identifikation von natürlichen und juristischen Personen und sonstigen Betroffenen herangezogene **Zahl**, die demjenigen, der identifiziert werden soll, **eindeutig zugeordnet** ist und hinsichtlich natürlicher Personen auch als Ausgangspunkt für die Ableitung von (wirtschafts)bereichsspezifischen Personenkennzeichen (§§ 9 und 14) benützt wird*

# Verwendung der Stammzahl

- Stammzahl steht auf jeder Bürgerkarte
  - in der Personenbindung
- Kann zwar ausgelesen werden
- Darf aber nur zur Berechnung der bereichsspezifischen Personenkennzeichen (bPK) verwendet werden
- Keine Speicherung!

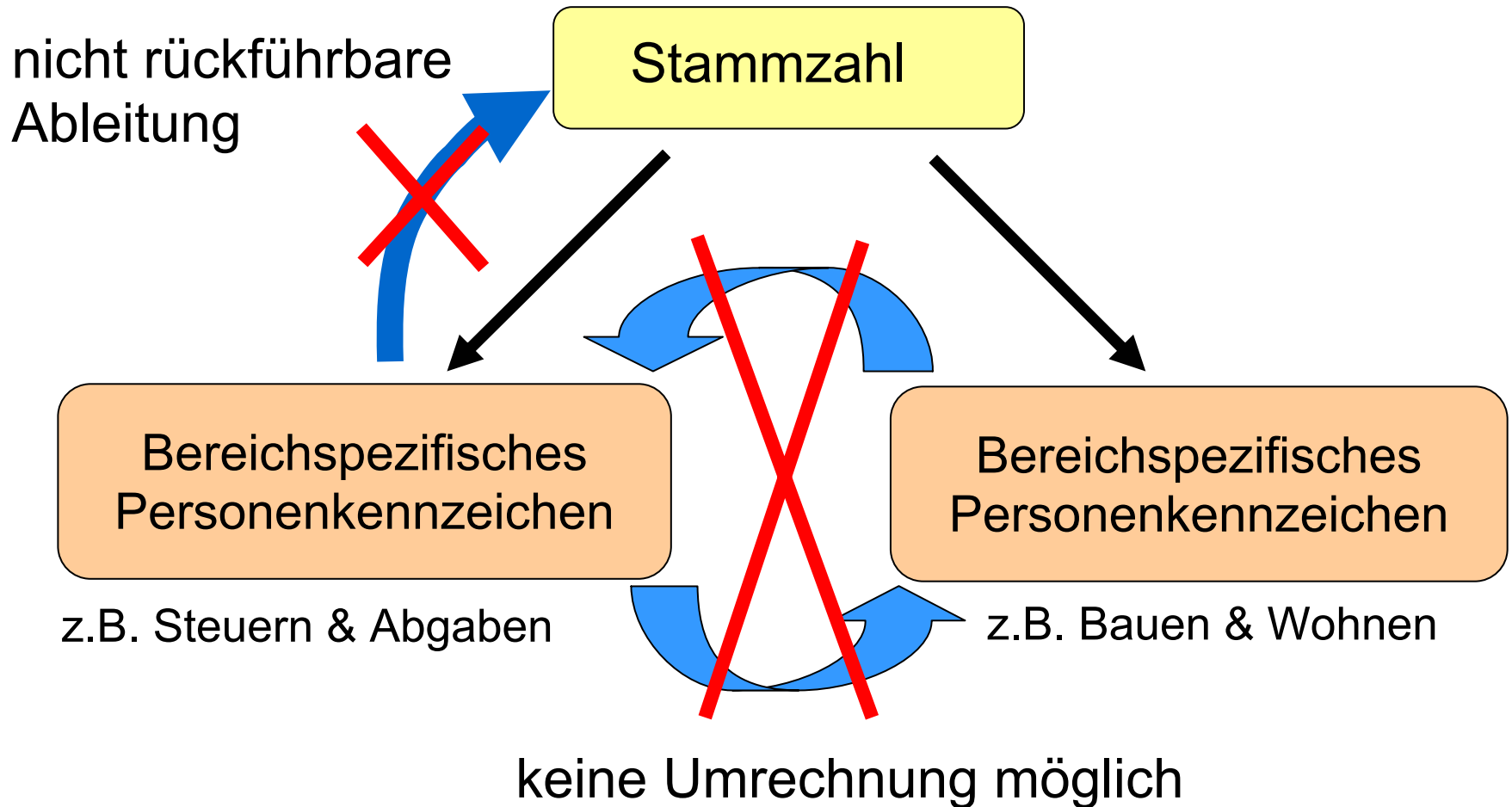
**Referenz:** EGovG §12



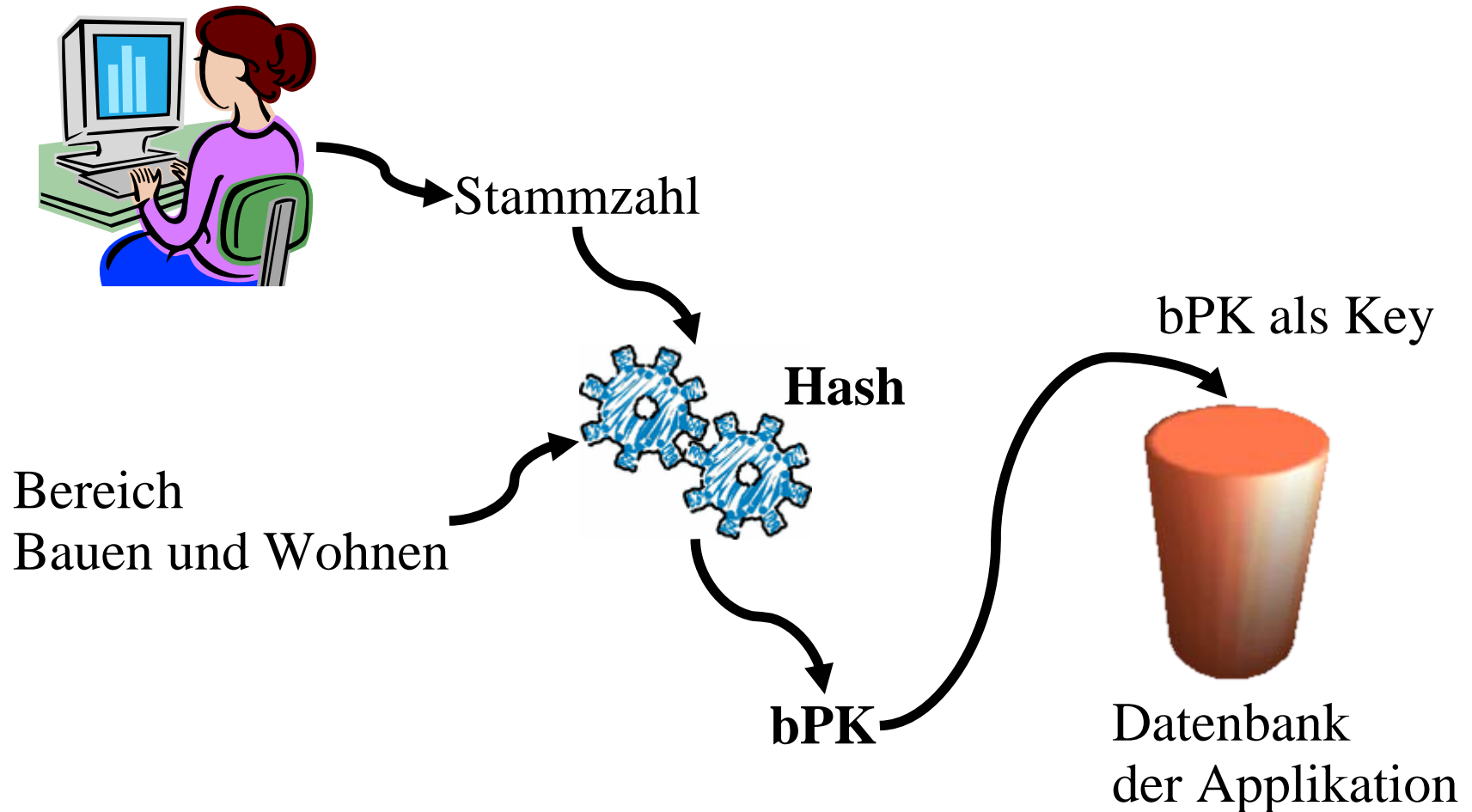
# Bereichsspezifisches Personenkennzeichen (bPK)

- § 9 (1) *Das bereichsspezifische Personenkennzeichen wird durch eine **Ableitung aus der Stammzahl** der betroffenen natürlichen Person gebildet. Die Identifikationsfunktion dieser Ableitung ist **auf jenen staatlichen Tätigkeitsbereich beschränkt**, dem die Datenanwendung zuzurechnen ist, in der das Personenkennzeichen verwendet werden soll.*
  
- (3) *Die zur Bildung des bPK eingesetzten mathematischen Verfahren (**Hash-Verfahren** über die Stammzahl und die Bereichskennung) werden von der Stammzahlenregisterbehörde festgelegt und [...] im Internet veröffentlicht.*

# Erzeugung des bPK



# Verwendung des bPK



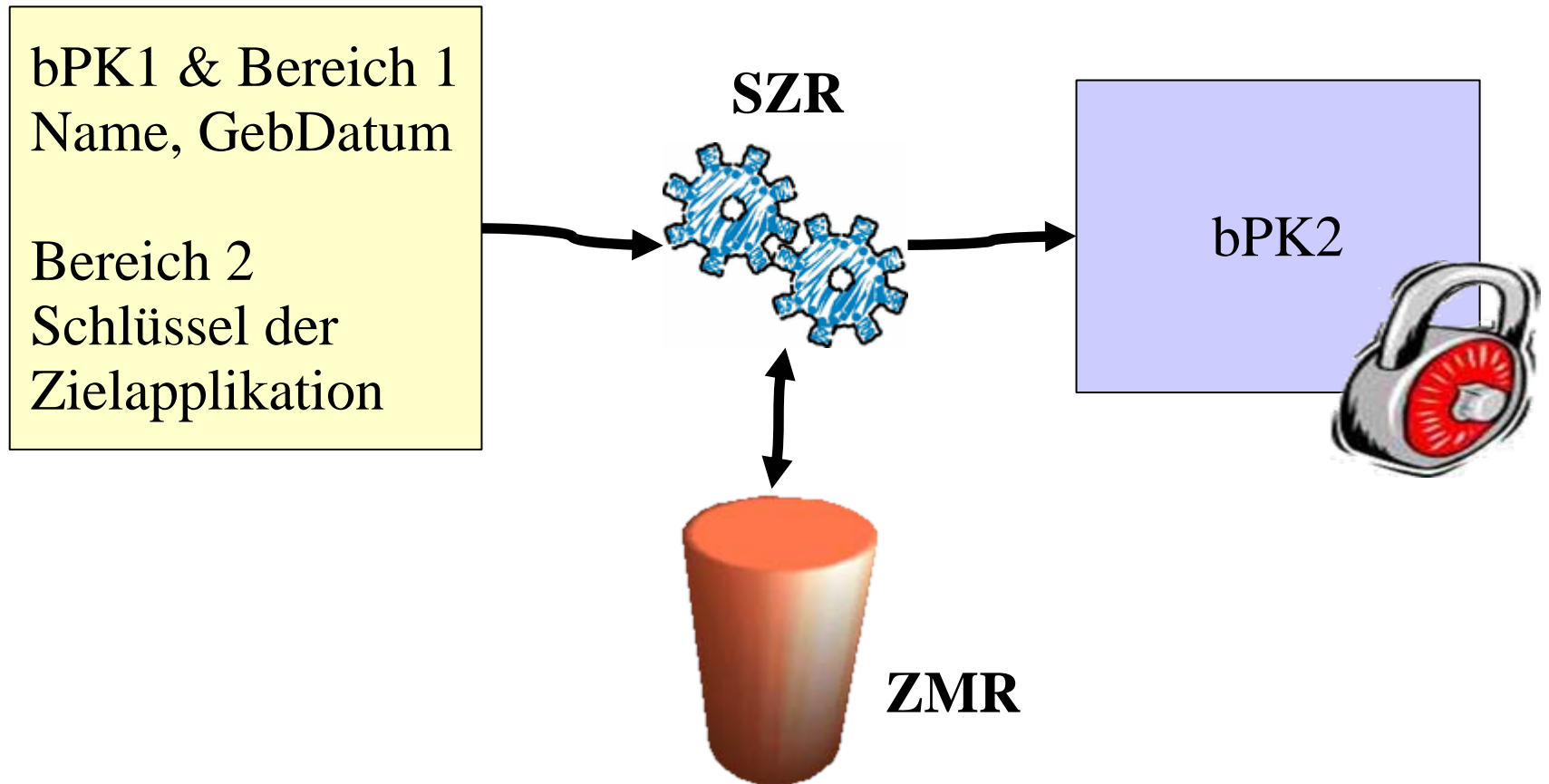
# bPK ohne Bürgerkarte

- bPK benötigt Stammzahl die auf Bürgerkarte ist
  
- Alternativ: Anfrage an das Stammzahlenregister (§10 (2) EGovG)
  - Input: ausreichend identifizierende Merkmale (Name, Geburtsdatum, Anschrift, ...) und gewünschter Bereich
  
  - Output: bPK für gewünschten Bereich

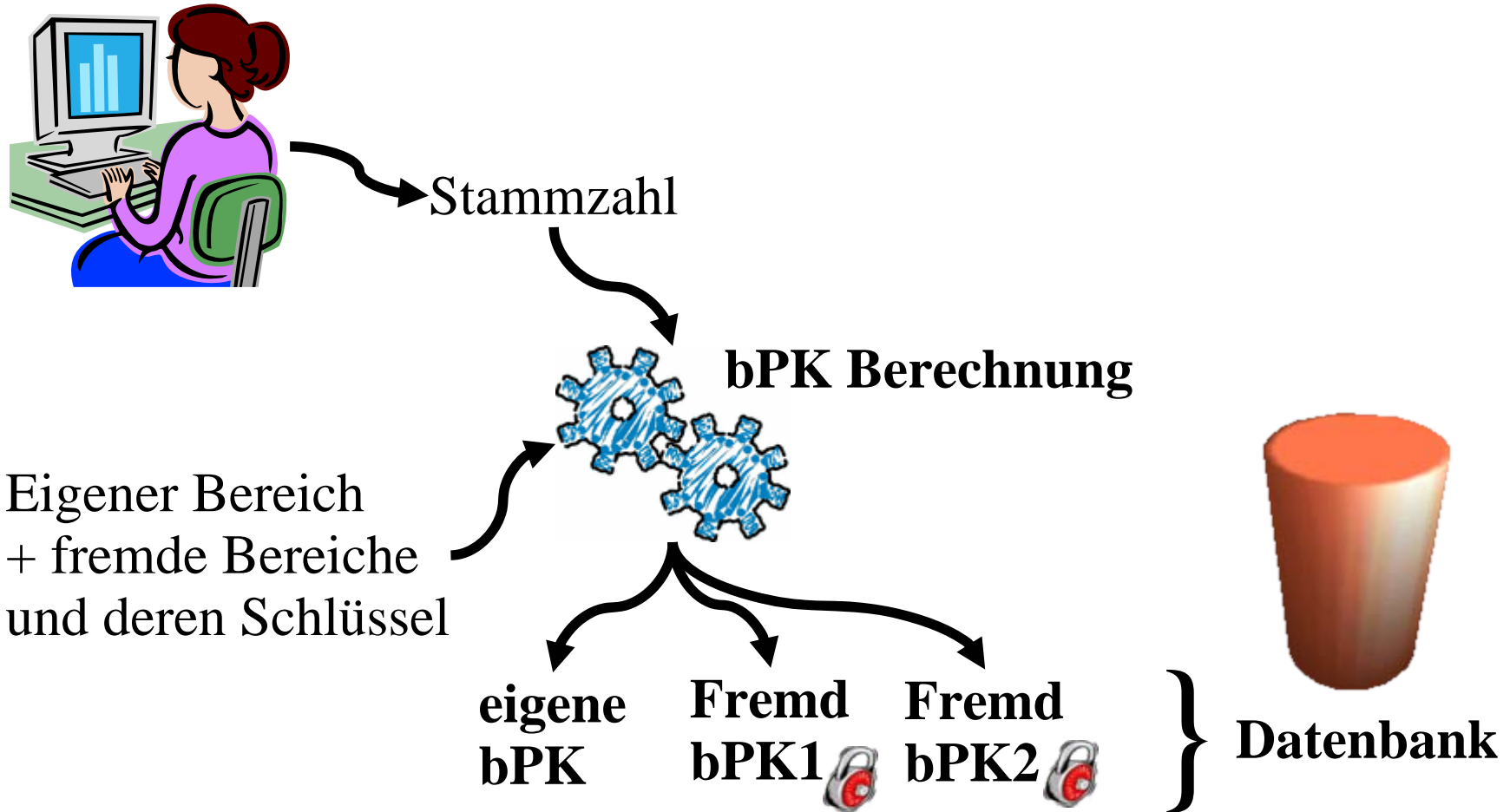
# Bereichsübergreifend

- Problem:  
bereichsübergreifende Verfahren,  
Querschnittsapplikationen benötigen  
unterschiedliche bPKs
  
- Lösung:
  - Umrechnung mithilfe des SZR (§10 EGovG)
  - Verschlüsselte bPKs: "Fremd-bPKs"  
(§13 (2) EGovG)

# Bereichsübergreifend (2)



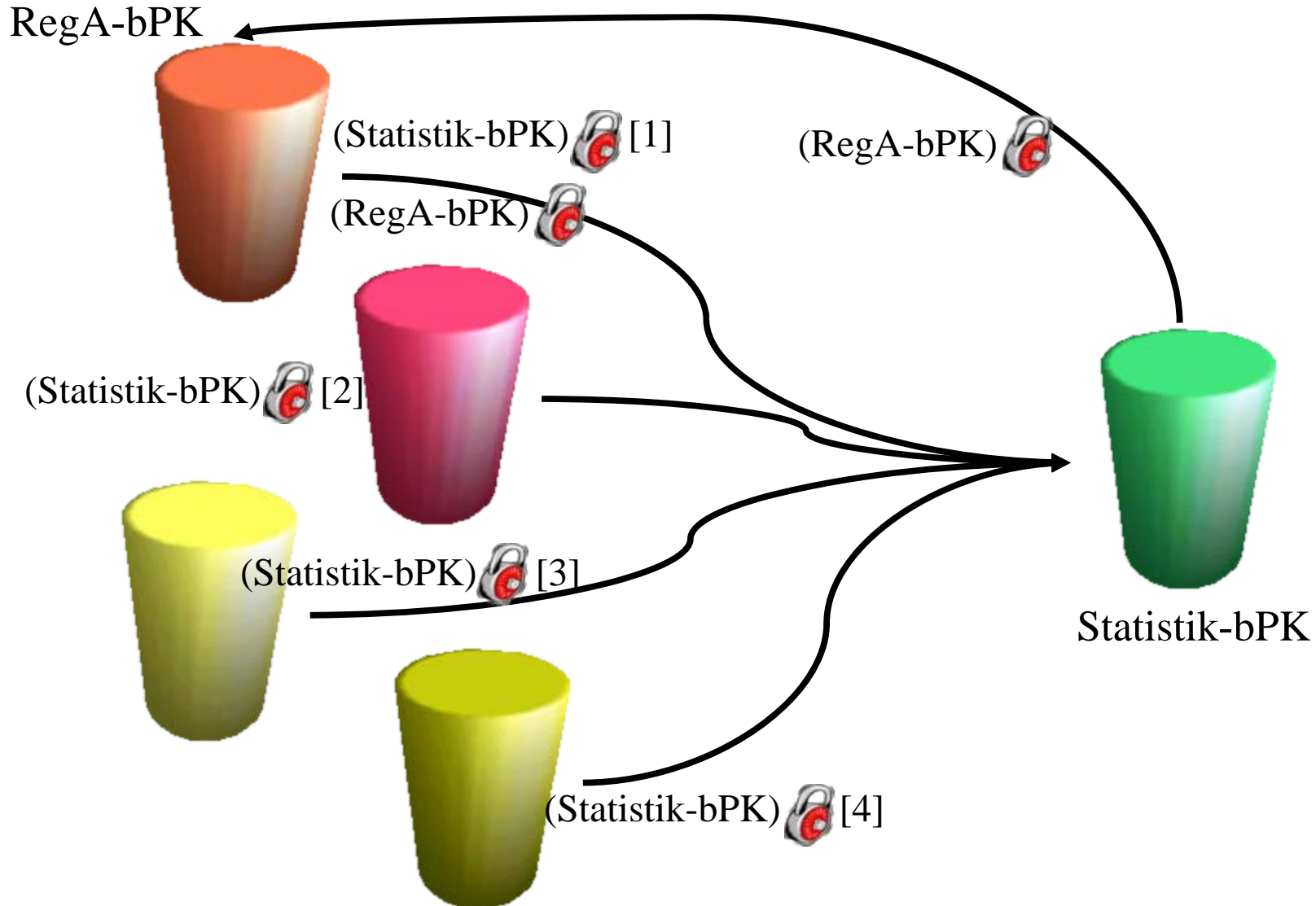
# Bereichsübergreifend (3)



# Beispiel: Krebsstatistik

- Aufgabenstellung
  - Statistische Erfassung von Krebserkrankungen
  - Vorfälle müssen passenden Personen zugeordnet werden
  - Anonym
- Lösung
  - Register speichert "Krebs-bPK"
  - Speichert keine Namen oder sonstiges
  - Anlieferung der Daten mit verschlüsselter "Krebs-bPK" (da Fremd-bPK aus Sicht der App)

# Beispiel: Registerzählung



# Zusammenfassung

- Stammzahl: Basiszahl für E-Government
  - darf "nicht" verwendet werden
  - Ausgangspunkt: Melderegister
  
- bPK: Bereichsableitung der Stammzahl
  - Erzeugung aus Stammzahl der Bürgerkarte
  - Erzeugung mithilfe des SZR
  - Umrechnung mithilfe des SZR
  - Speicherung von Fremd-bPKs in verschlüsselter Form möglich



# Danke für die Aufmerksamkeit

Fragen?



[Arno.Hollosi@cio.gv.at](mailto:Arno.Hollosi@cio.gv.at)  
Bereich IKT-Strategie

<http://www.cio.gv.at/>  
<http://www.guetesiegel.gv.at/>  
<http://labs.cio.gv.at/newsletter/>



# Erzeugung der Stammzahl

**ZMR-Zahl**

123456789012



*Verschlüsselung mit geheimen Schlüssel  
durch Stammzahlenregister*

**Stammzahl**

MDEyMzQ1Njc4OWFiY2RlZg==

**Referenz:** Bildung von Stammzahl und bPK

<http://www.cio.gv.at/it-infrastructure/sz-bpk/>

§6 (2) EGovG

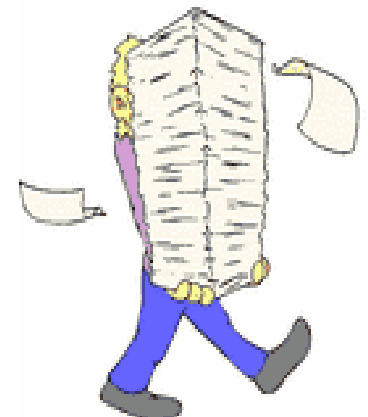
# bPK Erzeugung – Beispiel

- Stammzahl: *MDEyMzQ1Njc4OWFiY2RIZg==*
- Bereichskürzel: "*BAU*" (Bauen und Wohnen)
- Präfix: "*urn:publicid:gv.at:cdid+*"
- **SHA-1** über  
"*MDEyMzQ1Njc4OWFiY2RIZg==+urn:publicid:gv.at:cdid+BAU*"
- **bPK:**  
"*MswQO/UhO5RG+nR+klaOTsVY+CU=*"

**Referenz:** Bildung von Stammzahl und bPK, V1.0.2  
<http://www.cio.gv.at/it-infrastructure/sz-bpk/>

# Initialabgleich

- Migrationsweg für bestehende Datenbanken:  
wie kommt Applikation zu bPK?
  
- Initialabgleich durch Bulk-Anfrage ans SZR
  - Input: identifizierende Merkmale
  - Output: bPKs
  
- Nur manuelle Bulk-Abfrage in  
Abstimmung mit SZR
  - derzeit keine generische Schnittstelle
  - Datenbereinigung erfolgt manuell

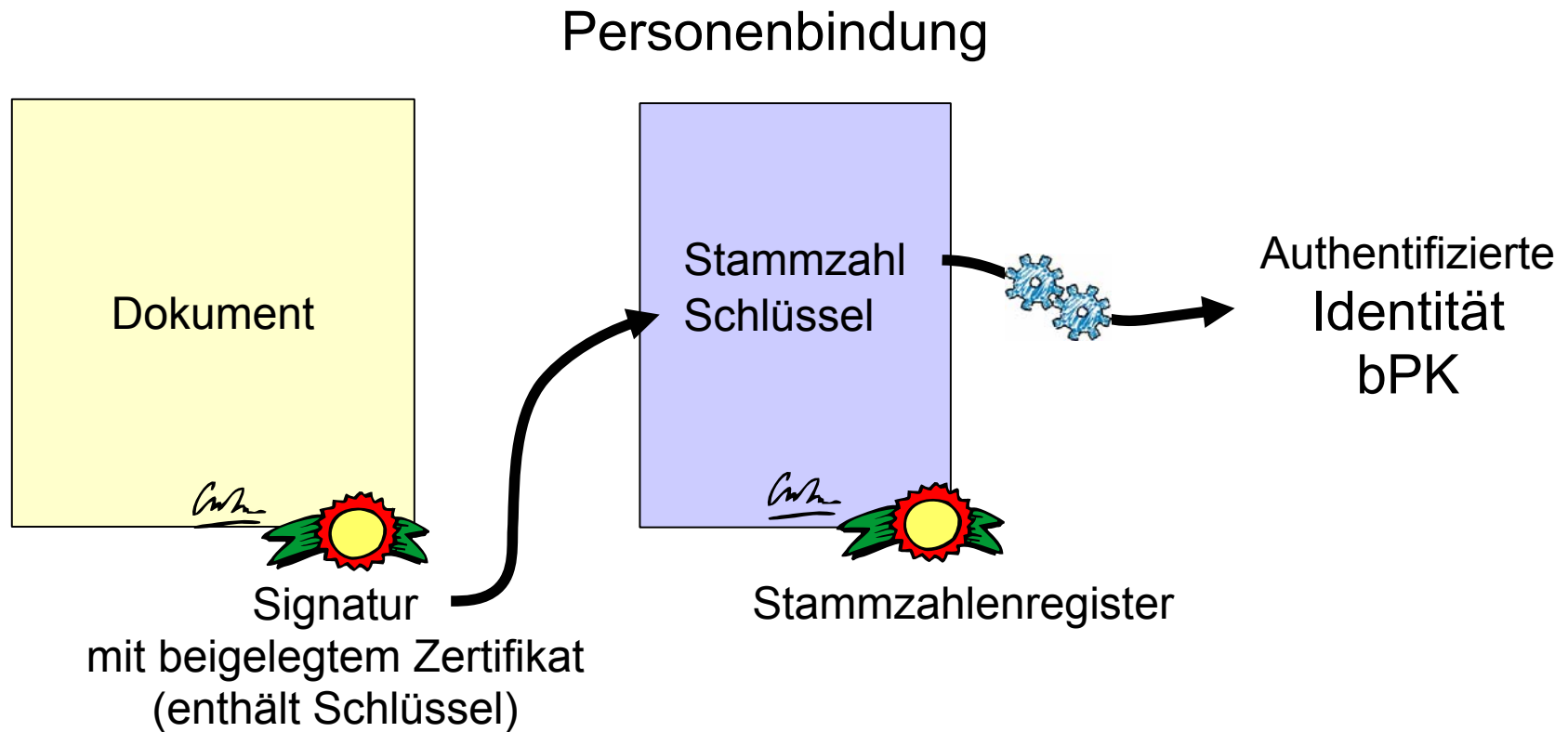


# Bürgerkarte

- §2 (10) EGovG: "Bürgerkarte":  
*die unabhängig von der Umsetzung auf unterschiedlichen technischen Komponenten gebildete logische Einheit, die eine elektronische Signatur mit einer Personenbindung (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie mit allenfalls vorhandenen Vollmachtsdaten verbindet.*
  
- *Ausprägung: Chipkarte oder Handy*
  - *auch andere Technologien*
  
- *Funktionen*
  - *Signatur, Personenbindung*



# Prüfungskette



# Stammzahlen für andere

- Nicht Meldepflichtige natürliche Personen
  - Ergänzungsregister mit freiwilliger Eintragung;  
aus Zahl wird Stammzahl analog berechnet
  
- Nicht natürliche Personen
  - Firmenbuch, Vereinsregister, Ergänzungsregister
  - Keine Ableitungen, Verschlüsselungen, etc.
  - Beispiel:  
Firmenbuchnummer  
== Stammzahl der Firma  
== bPK der Firma für alle Bereiche

# Vertretung

- EGovG §5 (1)  
*Soll die Bürgerkarte für vertretungsweise Anbringen verwendet werden, muss **auf der Bürgerkarte** des Vertreters ein Hinweis auf die Zulässigkeit der Vertretung eingetragen sein. Dies geschieht dadurch, dass die **Stammzahlenregisterbehörde***
  - 1. bei Nachweis eines aufrechten Vollmachtsverhältnisses bzw. Vorliegen gesetzlicher Stellvertretung **auf Antrag** des Vertreters die Stammzahl des Vertretenen und das Bestehen eines Vollmachtsverhältnisses mit allfälligen inhaltlichen und zeitlichen Beschränkungen auf der Bürgerkarte des Vertreters einträgt*

# Ablauf

- Die zu vertretende Person weist das aufrechte Vollmachtsverhältnis beim Stammzahlenregister nach (Webapplikation)
- Stammzahlenregister stellt Vollmacht aus
- (Benachrichtigung über) Vollmacht wird Vertreter zugestellt
- Vertreter trägt Vollmacht in die Bürgerkarte ein

# Ablauf (2)

- Vollautomatisch
  - Gewillkürte Vollmachten für natürliche Personen
  - für nicht-natürliche Personen  
(mit Unterstützung des zugehörigen Registers)
  
- Mit manueller Prüfung
  - Vorliegen gesetzlicher Stellvertretung
  - für nicht-natürliche Personen  
(falls keine Unterstützung vom zugehörigen Register)

# Berufsmäßige Parteienvertreter

- EGovG § 5. (1)  
*..., muss auf der Bürgerkarte des Vertreters ein Hinweis auf die Zulässigkeit der Vertretung eingetragen sein. Dies geschieht dadurch, dass die Stammzahlenregisterbehörde*  
  
*2. in den Fällen **berufsmäßiger Parteienvertretung**, in welchen ein besonderer Vollmachtsnachweis nicht erforderlich ist, auf der Bürgerkarte des Vertreters die Berechtigung zur berufsmäßigen Parteienvertretung elektronisch nachprüfbar anmerkt. Die elektronische Identifikation des Vertretenen erfolgt diesfalls gemäß § 10 Abs. 2.*

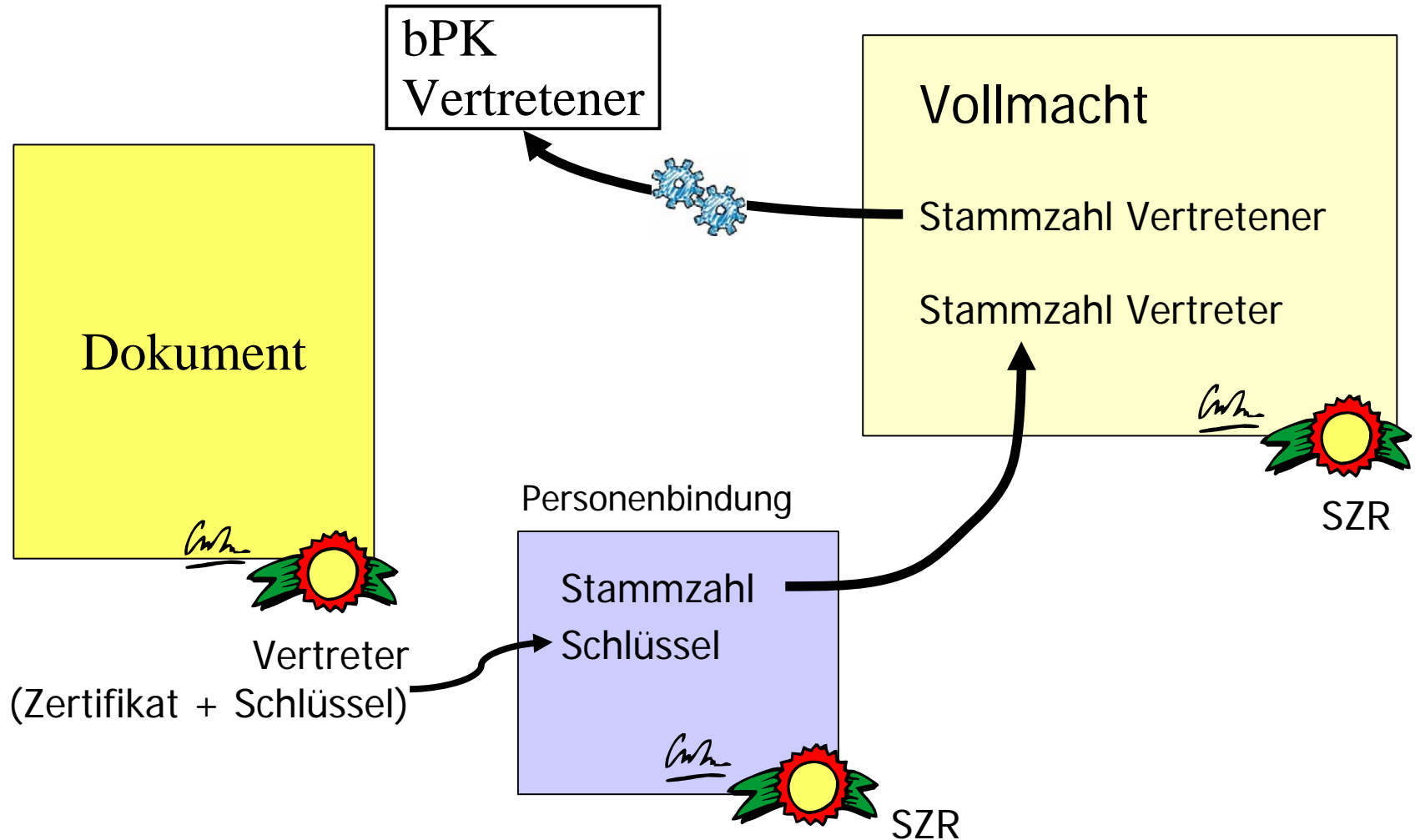
# Berufsmäßige Parteienvertretung

- Eintragung in Bürgerkarte dient als Nachweis
  
- Zwei Fälle
  - Nachweis für Applikation ausreichend
  - Applikation benötigt eindeutige Identität des Vertretenen (mittels bPK) – woher?
    - Antwort: Mit Nachweis kann (automatisch) Vollmacht bei SZR beantragt werden, welche die Stammzahl des Vertretenen enthält

# Inhalte einer Vollmacht

- Personen: Vertreter, Vertretener
- Ausstellungszeitpunkt
- Einschränkungen, Bedingungen
  - zeitlich
  - für bestimmte Bereiche oder Tätigkeiten
  - Recht auf weitere Delegation
- Widerrufsinformationen
- Signatur des Stammzahlenregisters

# Prüfungskette



## Vertretung (3)

□ *EGovG §5 (3)*

*Soweit bei Gemeinden oder Bezirksverwaltungsbehörden diese Dienstleistung eingerichtet ist, können [...] unabhängig von ihrer sachlichen und organisatorischen Zuständigkeit hiezu eigens ermächtigte **Organwalter für Betroffene** auf deren Verlangen Anträge in bürgerkartentauglichen **Verfahren** stellen.*

*Der Antrag wird mit Hilfe der Bürgerkarte des Organwalters gefertigt, die elektronische Identifikation des Betroffenen im Antrag erfolgt gemäß § 10 Abs. 2. Die generelle **Befugnis** des Organwalters zur Antragstellung für Betroffene muss aus dem **Signaturzertifikat** seiner Bürgerkarte hervorgehen*