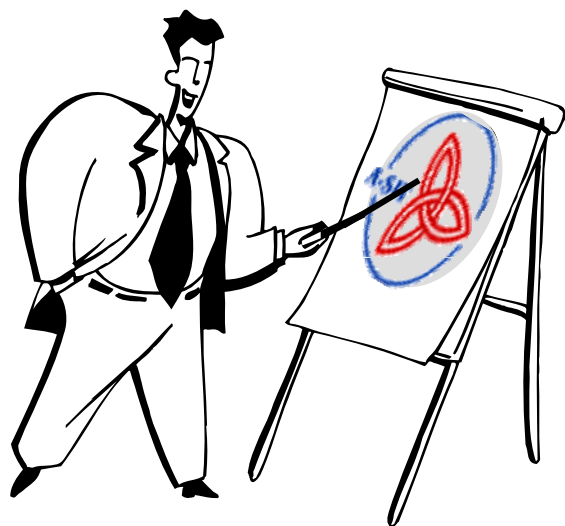


Identität und Rollen im österreichischen Gesundheitswesen: **eHealth-Verzeichnisdienst und GDA-Token**

Dipl.-Ing. Peter Danner

2. Konferenz der e-Health-Initiative Österreich
26. Januar 2007

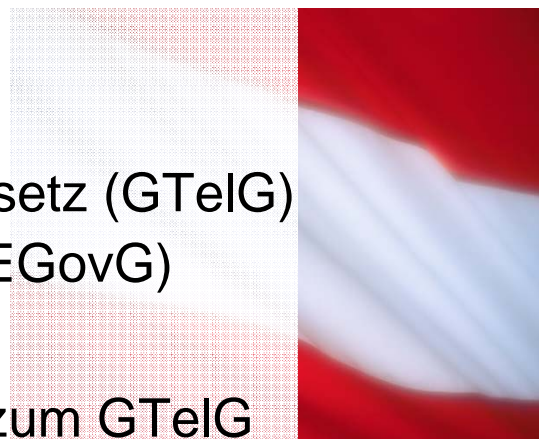
Inhalte



- Einleitung
 - GTelG, E-Government
 - HPI
- eHVD
 - Fakten
 - Positionierung
- GDA-Token
 - Aufbau
 - Prüfung , OTSP
 - Verwendung
- Ausblick / Zusammenfassung
 - MOA-ID, MOA-GDA

Anforderungen

- Identität und Rollen im österreichischen Gesundheitswesen
 - Identität
 - Gesundheitstelematikgesetz (GTeIG)
 - E-Government Gesetz (EGovG)
 - Rollen
 - Definiert in Verordnung zum GTeIG
- Kombination erforderlich
 - Token
 - Verzeichnis



Basis Gesundheitstelematikgesetz

3 Varianten der Identifikation eines GDA

– Explizite Bescheinigung

§ 4 (1) Der Nachweis der Identität ist durch Vorlage **einer elektronischen Bescheinigung** (Zertifikat), mit der die **in Übereinstimmung mit den §§ 3 bis 6 E-Government-Gesetz** festgestellte Identität der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters bestätigt wird, zu erbringen und zu prüfen. ..

– Verzeichnis

§ 4 (2) Der Nachweis gemäß Abs. 1 kann unterbleiben, wenn die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter **in den eHealth-Verzeichnisdienst** eingetragen ist und

– Automationsgestützt

§ 4 (3) Wird der elektronische Gesundheitsdatenaustausch ausschließlich programmgesteuert abgewickelt, ist – abweichend von Abs. 1 und 2 – der Nachweis der Identität **mittels Serverzertifikaten** zu erbringen und programmgesteuert zu prüfen. Serverzertifikate müssen den gemäß § 7 Abs. 5 festgelegten Mindestanforderungen entsprechen..

Synergie §4 (1) und §4 (2) GTeIG

3 Varianten der Identifikation eines GDA

- Explizite Bescheinigung

§ 4 (1) Der Nachweis der Identität ist durch Vorlage **einer elektronischen Bescheinigung** (Zertifikat) mit der die **in Übereinstimmung mit den §§ 3 bis 6 E-Government-Gesetz** festgestellte Identität der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters bestätigt wird, zu erbringen und zu prüfen. ..

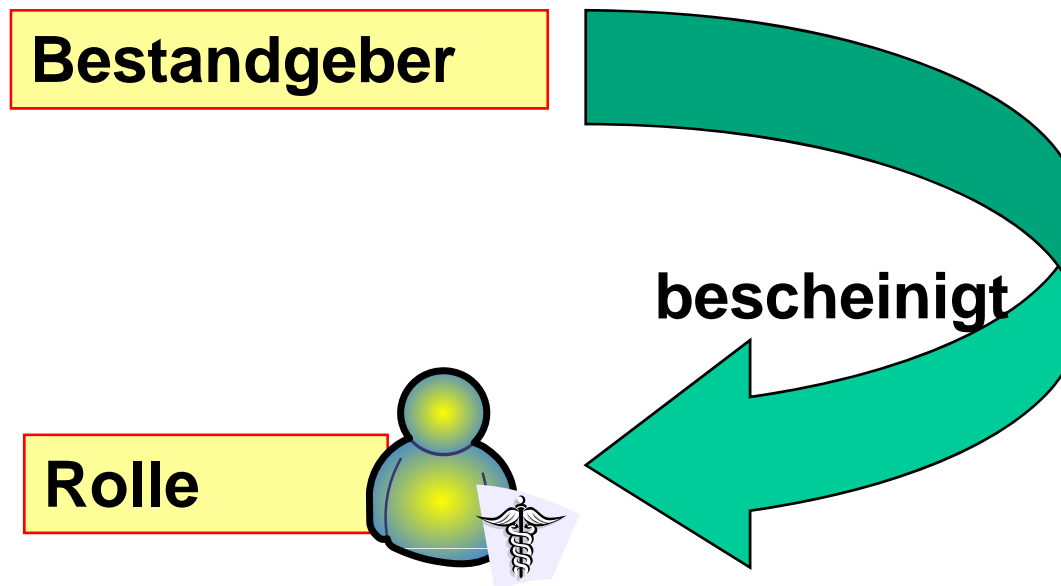
- Verzeichnis

§ 4 (2) Der Nachweis gemäß Abs. 1 kann unterbleiben, wenn die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter **in den eHealth-Verzeichnisdienst** eingetragen ist und

- Sinnvoll: Gemeinsame Datenstrukturen

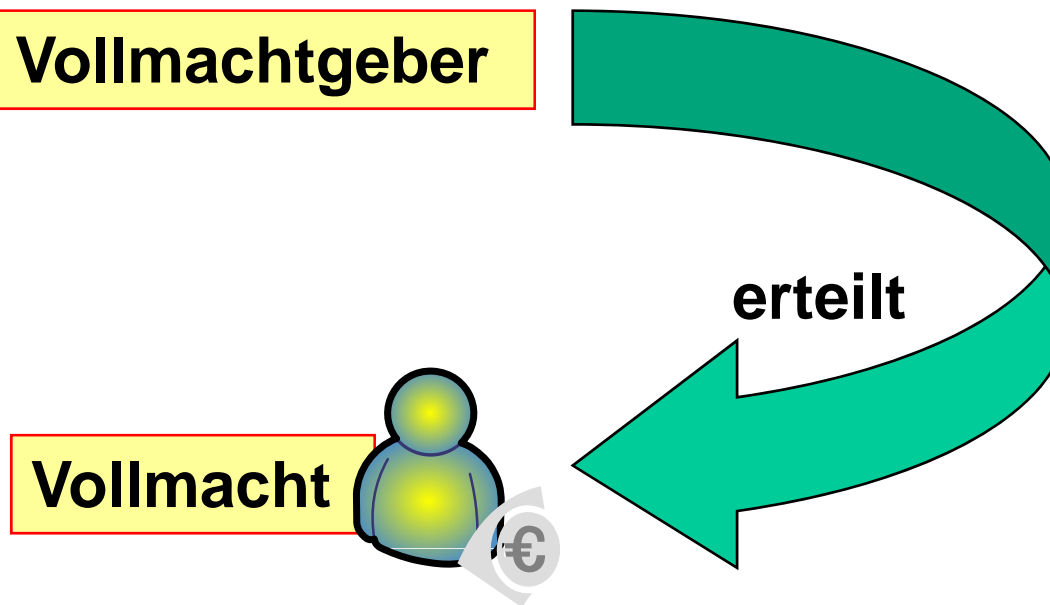
Synergie zu E-Government (1/2)

- Bescheinigung von Identität und Rolle



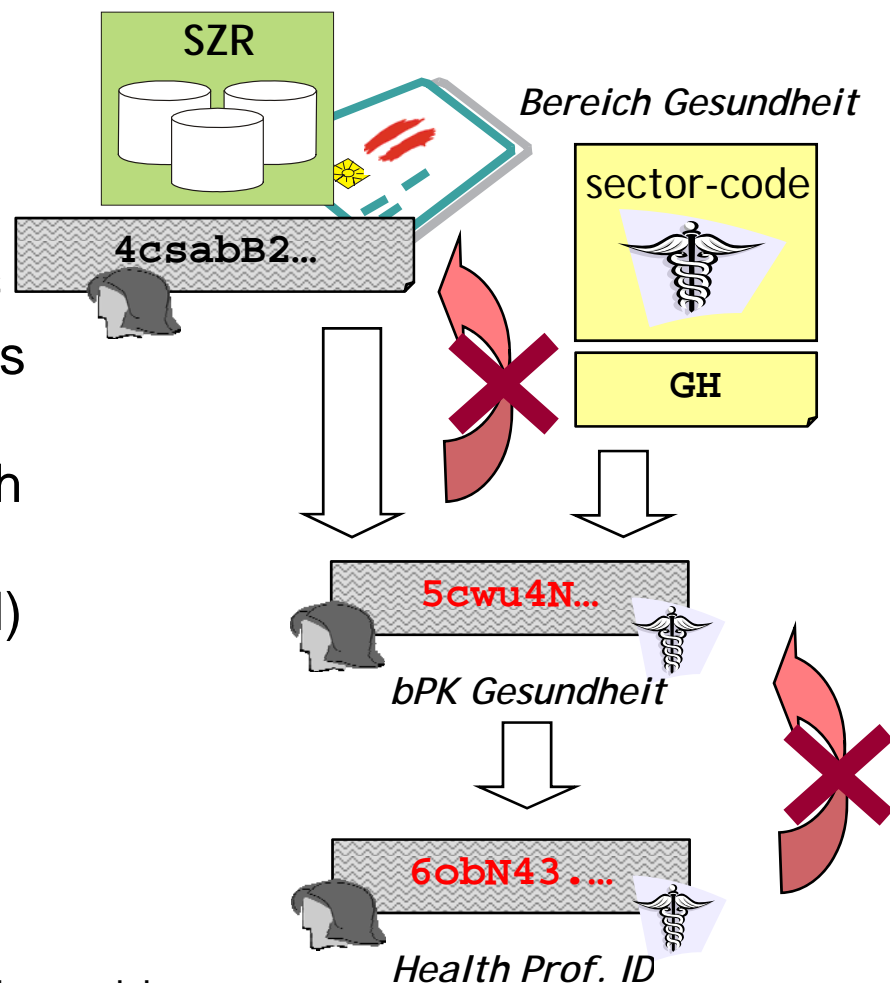
Synergie zu E-Government (2/2)

- Bescheinigung von Identität und Rolle



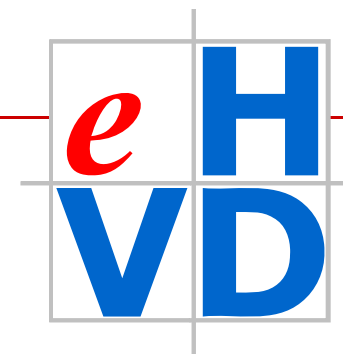
Health Professional Identifier - HPI


- bPK(*) darf nicht im privaten Bereich verwendet werden
 - Jedoch sinnvoll und notwendig (§ 4 (1) GTeIG), auf die eindeutige Identifikation aus Bürgerkarte abzustellen
 - Lebenslanger Identifikator auch für GDA
 - Weitere Ableitung der bPK(GH)



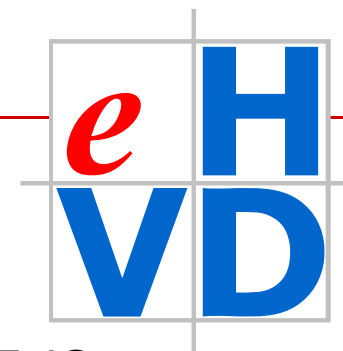
(*) bPK: bereichsspezifisches Personenkennzeichen

eHealth-Verzeichnisdienst (1/2)



- = Verzeichnis der Gesundheitsdiensteanbieter (GDA) samt deren Rollen
- Alternative zu Nachweis der Rolle (§ 4 GTeIG)
- **Web-Applikation** im BMGF
- Ziele
 - Bestätigung von Identität und Rolle für elektronische Kommunikation mit Gesundheitsdaten
 - Qualifizierter Datenzugriff
 - Nutzung im Rahmen eines künftigen Gesundheitsportals
 - Anhebung der Datensicherheit
 - Gesicherter, staatenübergreifender Datenaustausch 
- IST-Stand
 - Zugang (z.B. Antrag, Abfrage, Bestätigung, Freigabe) für natürliche Personen über BKU^(*)

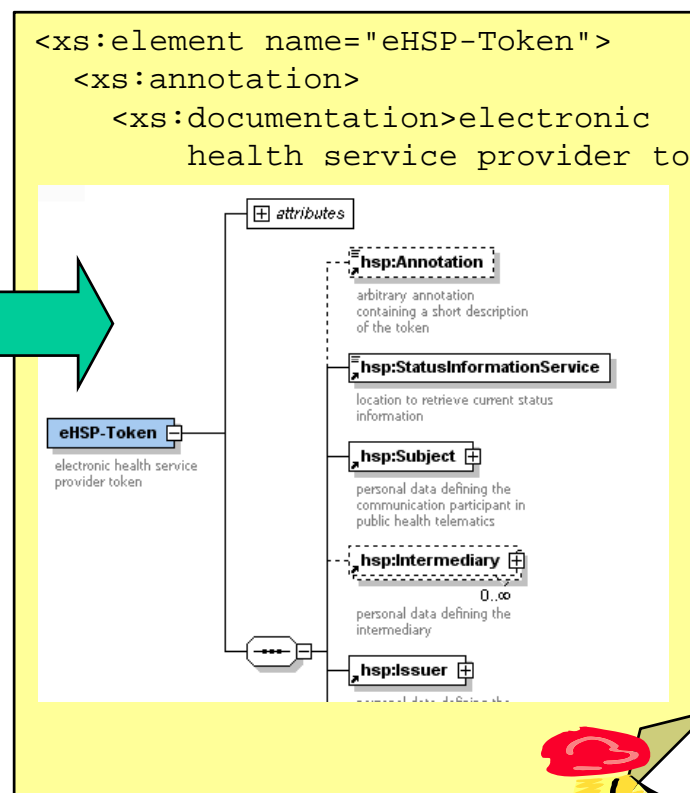
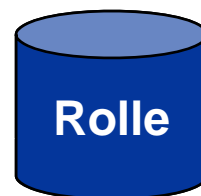
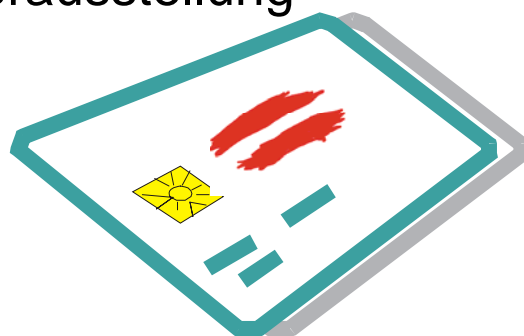
eHealth-Verzeichnisdienst (2/2)



- Aufnahme in den eHVD nur auf Antrag eines GDA
 - **Freiwilligkeit**
 - Bei Registrierung im eHVD Aufnahme weiterer, im § 10 GTeIG genannter, Daten
 - E-Government konformer Prozess
- Bescheinigung = authentische Bestätigung
 - **Verwendung auch außerhalb** der Kontexts eHVD
 - Elektronische Zustellung
- Verzeichnis und Auskunftstelle
 - Suche im eHVD
 - Überprüfung eines GDA-Tokens
 - Tägliche Replikation
- Positionierung
 - BMGF ist Trustholder
 - österreichweit, institutionenübergreifend
 - entsprechend der Forderung im eHI Strategiebericht 2005

GDA Token

- XML-Datenstruktur
- enthält
 - Eindeutige Token-ID
 - Identifikation
 - HPI Health Professional Identifier „abgeleitete bPK“
 - Rolle als OID+Beschreibung
 - Gültigkeitsdauer
 - Statusinformationsservice-URL
 - Bestandgeber + Signatur
 - Ggf. „Weiterausstellung“



Rollen - OID

- Standardisierte Objekt-Bezeichner
- In Verordnung zum GTeIG festgelegt
 - Bestimmte Hierarchien weiter ableitbar
- Eindeutige Beschreibung der Rollen
 - root-OID = {1.2.040.0.22}; Bezeichner: "public-health"
 - OID (präfix) = {1.2.040.0.22.1}; Bezeichner: "ehvd,,
- Beispiele:
 - 1.2.040.0.22.1.2.3 Gesundheitspsychologin/Gesundheitspsychologe
 - 1.2.040.0.22.1.2.4 Hebamme
- Abhängige Rollen durch OIDConstraints möglich

```
- <Role>
- <OID>
  <pr:Value>1.2.040.0.22.1.2.3.77</pr:Value>
  <pr:Type>urn:publicid:gv.at:ehspoid</pr:Type>
</OID>
- <Description>
  <TextualDescription>Gesundheitspsychologin/G
</Description>
```

GDA-Token Widderrufsprüfung

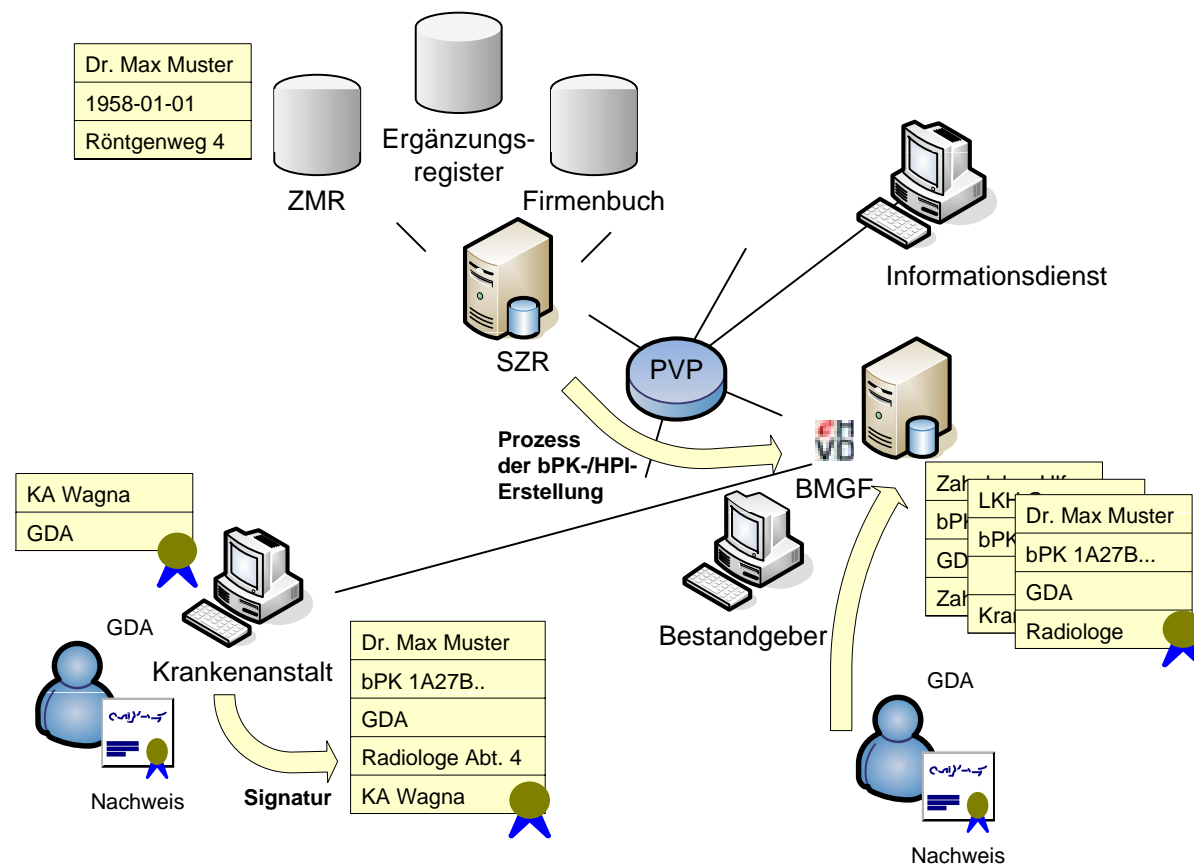
- Online Token Status Protocol - OTSP
 - Online Protokoll
 - angelehnt an OCSP (*) (RFC 2560)
 - vgl. OMSP(**)
 - XML-Requests über HTTP-Anfragen
 - Signierte Antworten
 - Prüfservice = OTSP Responder
 - Stati:
 - active (Token gültig)
 - revoked (Token widerrufen)
 - suspended (Token ruhend gestellt)
 - unknown (Token unbekannt)

(*) OCSP: Online Certificate Status Protocol

(**) OMSP: Online Mandate Status Protocol

Identität und Rollen Infrastruktur

Player im Ausstellungsprozess



Verwendung von GDA-Token

The image shows two overlapping software windows. The background window is titled 'GDA-Token Verwaltung' and displays a profile management interface. It includes a dropdown menu for 'Profil' (set to 'Profil 1'), buttons for 'Neues Profil ...' and 'Speichern', and sections for 'Verfügbare GDA-Token' (listing 'Psychotherapeut2' and 'Psychotherapeut1') and 'Ausgewähltes GDA-Token' (listing 'KlinPsychologe'). There are also buttons for moving tokens between lists and a checkbox for 'ausgewähltes Profil standardmäßig aktivieren'. The foreground window is titled 'trustview 2.1.1' and shows a digital signature process. It features the 'DIGITAL AUSTRIA' logo and the text 'Dokument signieren it solution'. The main content is titled 'Signatur der Anmeldedaten' and contains a signed statement: 'Mit meiner elektronischen Signatur beantrage ich, Peter Christian Danner, geboren am 28.10.1971, in der Rolle als Psychotherapeutin/Psychotherapeut (OID *= 1.2.040.0.22.1.2.1.13), den Zugang zur gesicherten Anwendung.' Below this, it shows the date and time '25.01.2007, 07:18:33' and the HPI value '+eK0hL5RBZjWy+FEG/LSziwXnts='. At the bottom, there are buttons for 'Beenden', 'Zertifikat', and a field for '6+ stellige Signatur PIN' with an 'OK' button.

Zusammenfassung / Ausblick

- Erhöhung der Datensicherheit im Umgang mit Gesundheitsdaten
 - Zugang personalisiert und mit Rollen
 - Einfache Initiierung verschlüsselter Kommunikation
- Einfache System-Adaption durch Verwendung von zur Verfügung stehenden Software-Modulen
 - Eindeutige Authentifikation mit Rollen durch Kombination von
 - MOA-ID 1.4(*)
 - MOA-GDA zur Prüfung von GDA-Token (Rollen)
- Durch „Weiterausstellung“ von GDA-Token Berechtigungen noch feiner auflösbar

Danke für Ihre Aufmerksamkeit!

<http://www.ehvd.at>

Dipl.-Ing. Peter Danner

Zentrum für sichere Informationstechnologie - Austria

+43 316 873-5537

peter.danner@a-sit.at