ecard

The Austrian e-card - Part of the eGov-Strategy

Dipl.-Ing. Heinz Otter

ITAPA - Conference, Bratislava, 19.10.2004

Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H.
Schiffamtsgasse 15, A-1020 Wien

SVC: „Social Security Chipcard - Company“

ecard

- „**S**ozial**v**ersicherungs-**C**hipkarten Betriebs- und Errichtungsges.m.b.H.“ establishes the project and is in charge to operate the system
- established February 24th, 2001
- 100% in the position of the „Main Association of Austrian Social Security Institutions“

The „SVC - Company“

ecard

- The **SVC** is **system integrator**
  Implements the „**E**lectronic **A**dministration **S**ystem“ **(ELSY)** on behalf of the „Main Association of Austrian Social Security Institutions“
- First Step:
  Substitution of the health insurance vouchers by a **smart card.**
- Mission of the company:
  Establishment, implementation, operation and **extension** of **ELSY***)
  using a **multi-applicative smart card system** within the field of **Austrian Social Security**.

*) according to §§ 31a to 31c ASVG (i.e. General Law on Social Insurance)

SVC

Vision: e-card of the Austrian Social Security in Operation...

ecard

Hospitals

Medical Practices

Out-patient Clinics

Pharmacies

Ambulance Services

Dentists

Social Security Services

Keycard for eGov-Applications

SVC

Present Process: „Consultation of a Doctor“

ecard

Employer

Issue of health insurance vouchers

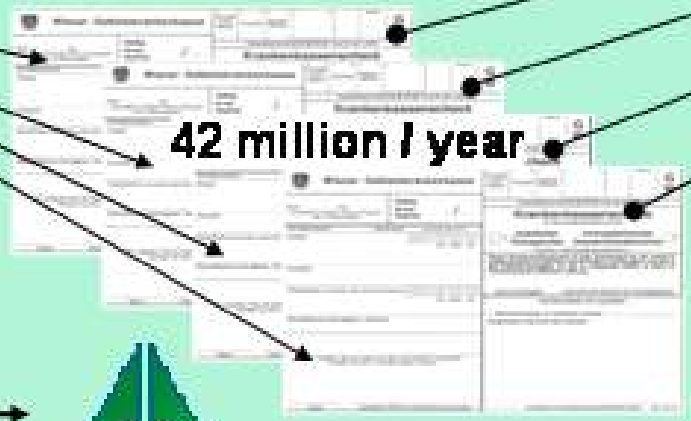
Employee

Physician

(1)

Insurance status:
Registration &
Deregistration process

(2)



42 million / year

(3)

Sending of health insurance vouchers to Social Security Institutions for .....

Computer System(s)
Social Security Institutions

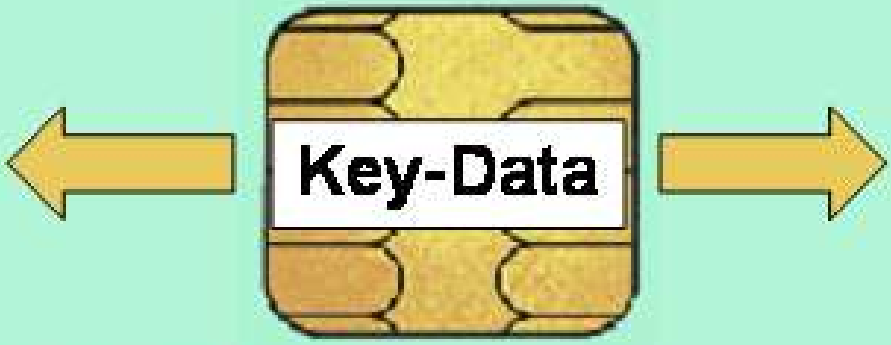
(4)

....**Accounting**

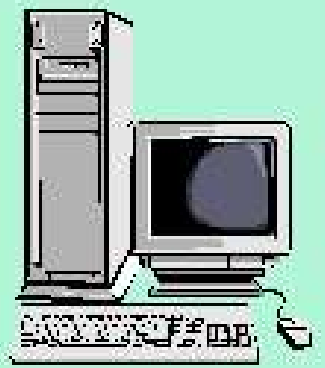
Basic Application: „Substitution of all Health Insurance Vouchers in Use“

ecard

Substitution of about **42 million health insurance vouchers** per year



Supply of **8 million insured** with e-cards



Integration of about **12.000 contractual partners**

- Software clients for medical practices
- chipcard readers
- via „Medical Practice Unit (MPU)"

Requirements to the Compound System

ecard

Legal Provisions:

- Design of the e-card as a „**Keycard**"
- Access to **personal data** after approval of the cardholder (§31a (2) ASVG)
- **Reloadability** of health data on the smart card
- The e-card system shall support the **transparency** of medical services and costs
- Acceptance of other cards with „Citizen Card Functionality" (i.e. prepared for eGovernment).

System Requirements

ecard

General Provisions:

- „**Medical Practice Unit**":
  All interfaces to existing local IT-Infrastructure and to data networks will be standardized and supported by this „Unit"
- **Technological sphere** of the **insured**:
  Consideration of existing degree of IT-utilization (➔ 2005)
- **Realization** of **system components**:
  Based on common technological and industrial standards
- **Practical application** of the **project experiences** in other european countries (e.g. DE, SL, SP, IT)
- Aspects of **interoperability**:
  Development in Europe, e.g. EHIC, Netc@rds

System Requirements

ecard

Use of achieved technological development:

- Capability for **Citizen Card** Applications:
  electronic signature(s) according to SigG/SigV & VW-SigV
- Access to **e-applications** of **Social Security**:
  via **eSV-Portal** (services of all 25 Soc.Sec. - Institutions)
- **Electronic accounting** of physicians:
  settled by law since January 1st, 2003
- Availability of **data networks** with sufficient performance as well as motivating charges (useable also for value added services)

Openness of the System

ecard

- **Modification** of the **„Conditions for Claim"- rules**:
  Requires **software-updates** by the operating company, which is specifically supported by the online-system
- **Loadability of new applications:**
  Post Issuance Personalisation and downloading of data, data structures and cryptographic key-files to the e-card
- **Innovation and migration:**
  Simultaneous operation of **several „generations" of smart cards** with different scope of applications

Security of the e-card: Basic Aspects

ecard

- **Access key (token)** is **unique** within the system
- **Lost token** are locked systemwide
- **Processor-Chip:** sufficiently **copy-safe**
- **Security-levels of different strength** depending on the application, usefully combined with
  - ➔ cryptographic methods
  - ➔ electronic signature
  - ➔ PIN / identification feature,

  which are implemented in the **e-card.**

SVC

Future Process: „Consultation of a Doctor“

ecard

Employee

Employer

Physician

(1)
Insurance status:
Registration -
Deregistration

Computer System(s)
Social Security Instit.

(2)

(3)

(4)
Accounting via
physician's EDP

Claim

Data

Online
Electronic Data
Transmission

„Consultation Server
Center" for e-cards

Online Check of Claim
(SV-Signature protected)

The Keycard-Principle

ecard

- Physically the **e-card** corresponds to an **intelligent token** which represents the **access key** to **system-based services and data**.
- The **e-card** is principally **not** a carrier of application software functions.
- The **e-card** contains **identification data** which are required for the **access authorization** to applications.

SVC

Electronic Signatures of the e-card

ecard

3 signature-applications on card:

- **Administrative electronic signature** (according to VW-SigV)
  for eGovernment and eCommerce applications

„eGov“

- **Advanced electronic signature**
  for general applications, where no secure signature is required

„eSocSec“

- **Social Security Signature**
  for secure electronic transmission in the field of „substitution of health insurance vouchers“ (KSE) and eSV

e-card: Part of the Austrian E-Government Strategy

ecard

- **Administrative Electronic Signature**
  (see VW-SigV, valid as a „Qualified Signature“ until 12/2007)
- **Unique Identification of the Signatory: Identity Link**
  = data structure binding a citizen‘s certificate to a person‘s identity (Base Identification Number, Sector Specific Personal Identifier)
- **Client-Software „Citizen Card - Environment“:**
  High level interface „Security Layer“, software provided by the Austrian Federal Government, available for everybody via download: www.cio.gv.at/identity/bku

eGov – Strategy Security Layer

ecard

eGov - Application

Security Layer

Citizen Card Environment

PIN Input

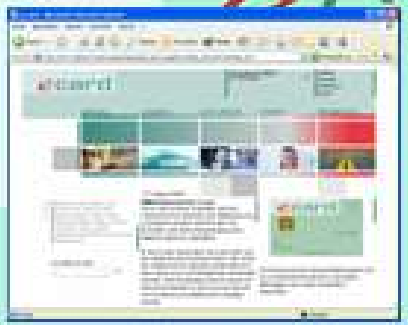
Hash-Function

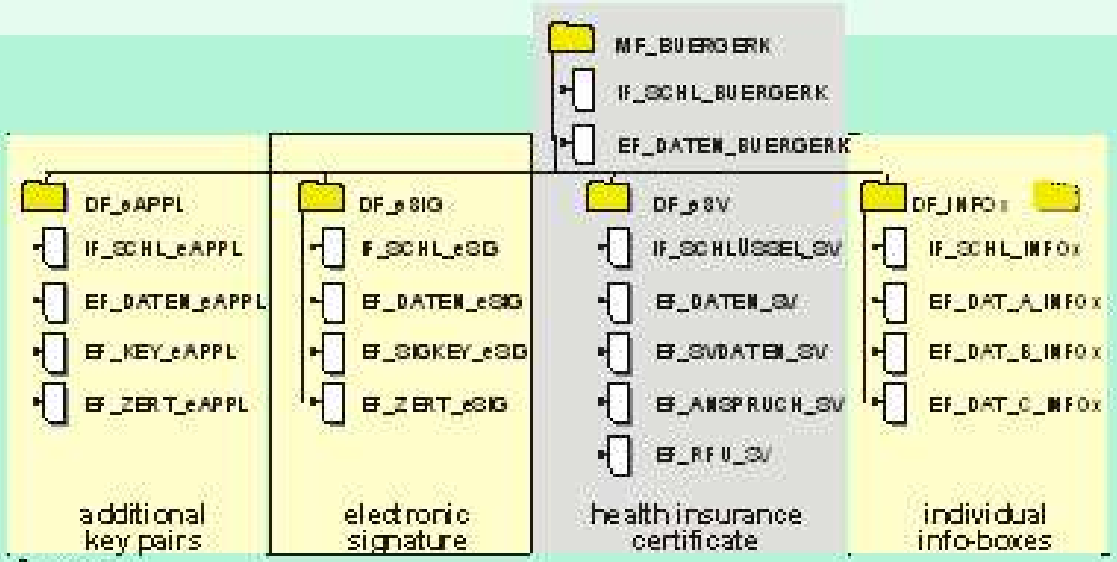
Trusted Viewer

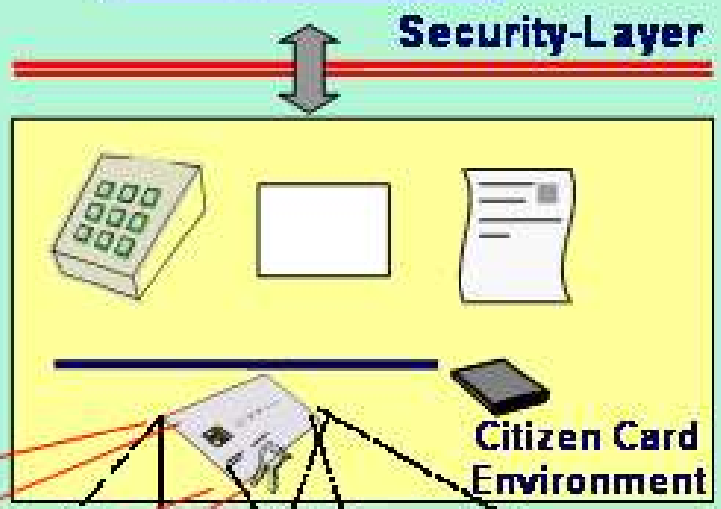
Card Interface (e.g. PKCS#11)

Add on Memory

eGov – Strategy
Technology Independence



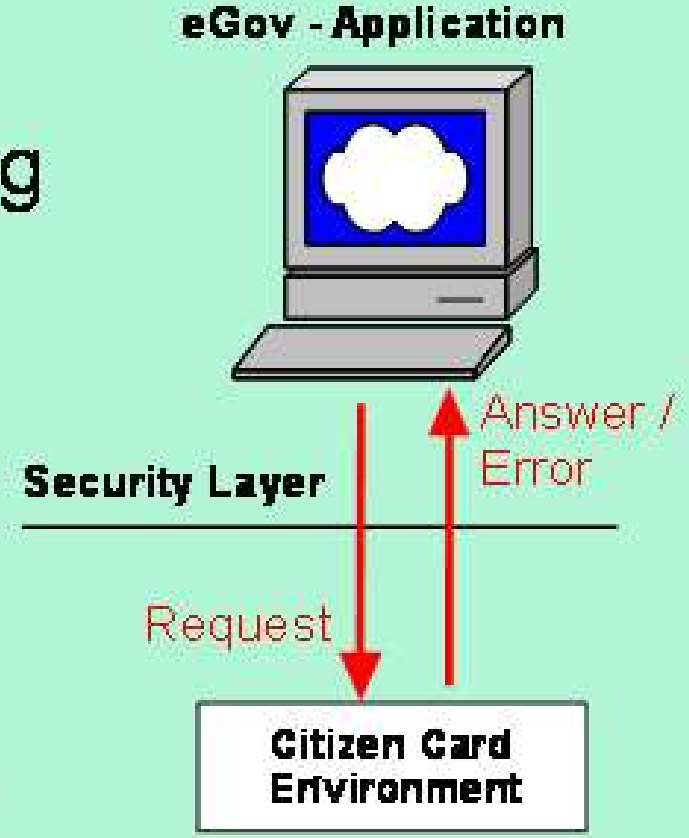




eGov – Strategy Protocol Structure

ecard

- Simple Request / Answer - Dialog
  - Application sends Request
    - e.g. „Sign Document“
  - Security-Capsule reacts with
    - Answer - or
    - Error message
- Code of Protocol Elements: XML



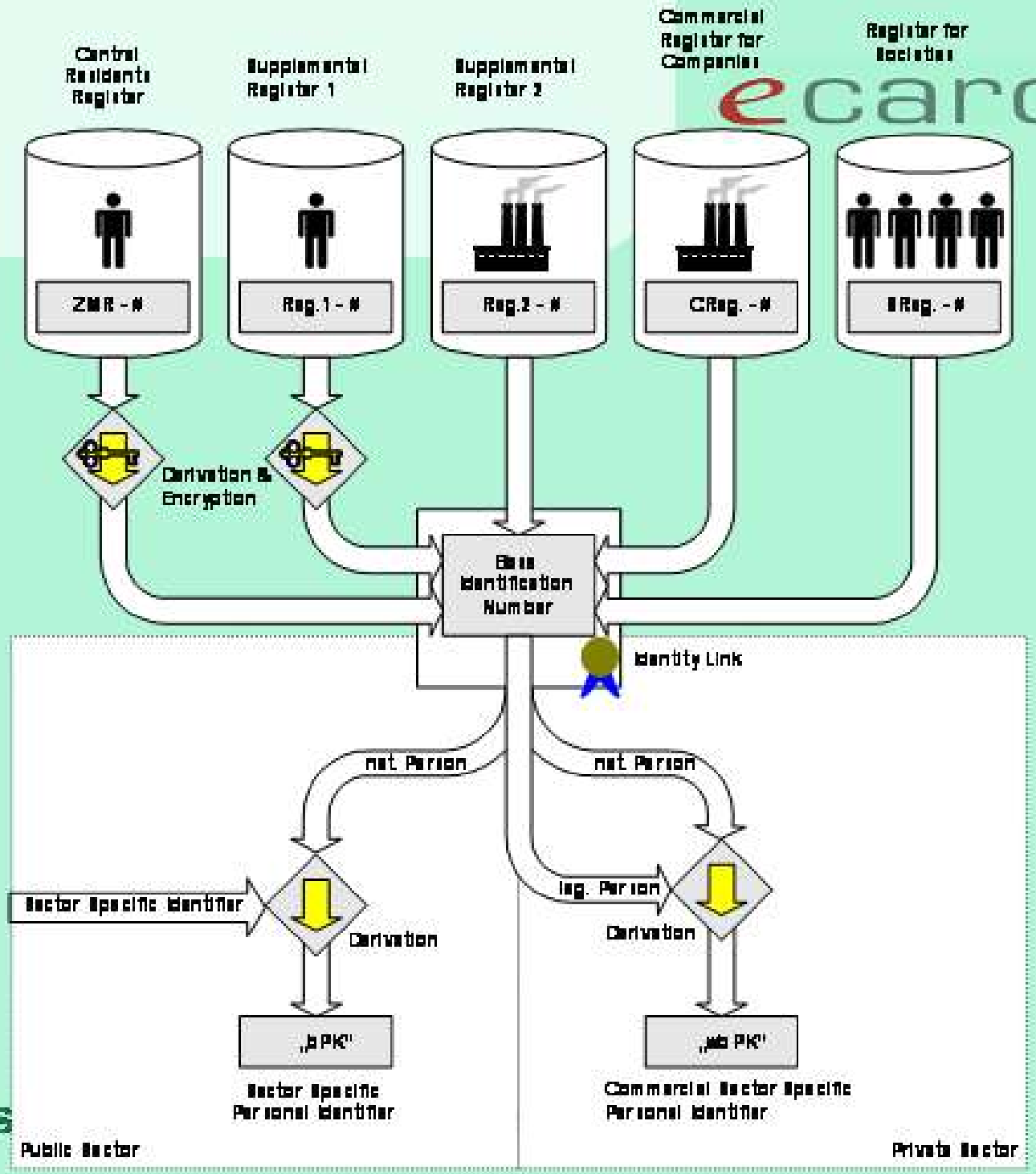
Austrian E-Government: The „Identity Link“

ecard

- **„ZMR“ = Citizen‘s Identification Number**
  (supplied by „Residents Register“)
- **„SZ“ = Base Identification Number**
  (derived by strong encryption of ZMR, identifies each person registered in Austria uniquely)
- **„BKZ“ = Sector Specific Identifier**
  (identifies different Applications of E-Government)
- **„bPK“ = Sector Specific Personal Identifier**
  (cryptographic derivation out of „SZ & BKZ“)

SVC

Derivation of the „Sector Specific Personal Identifier“ out of several registers



The Aus

eGov – Strategy
Identity Link

ecard

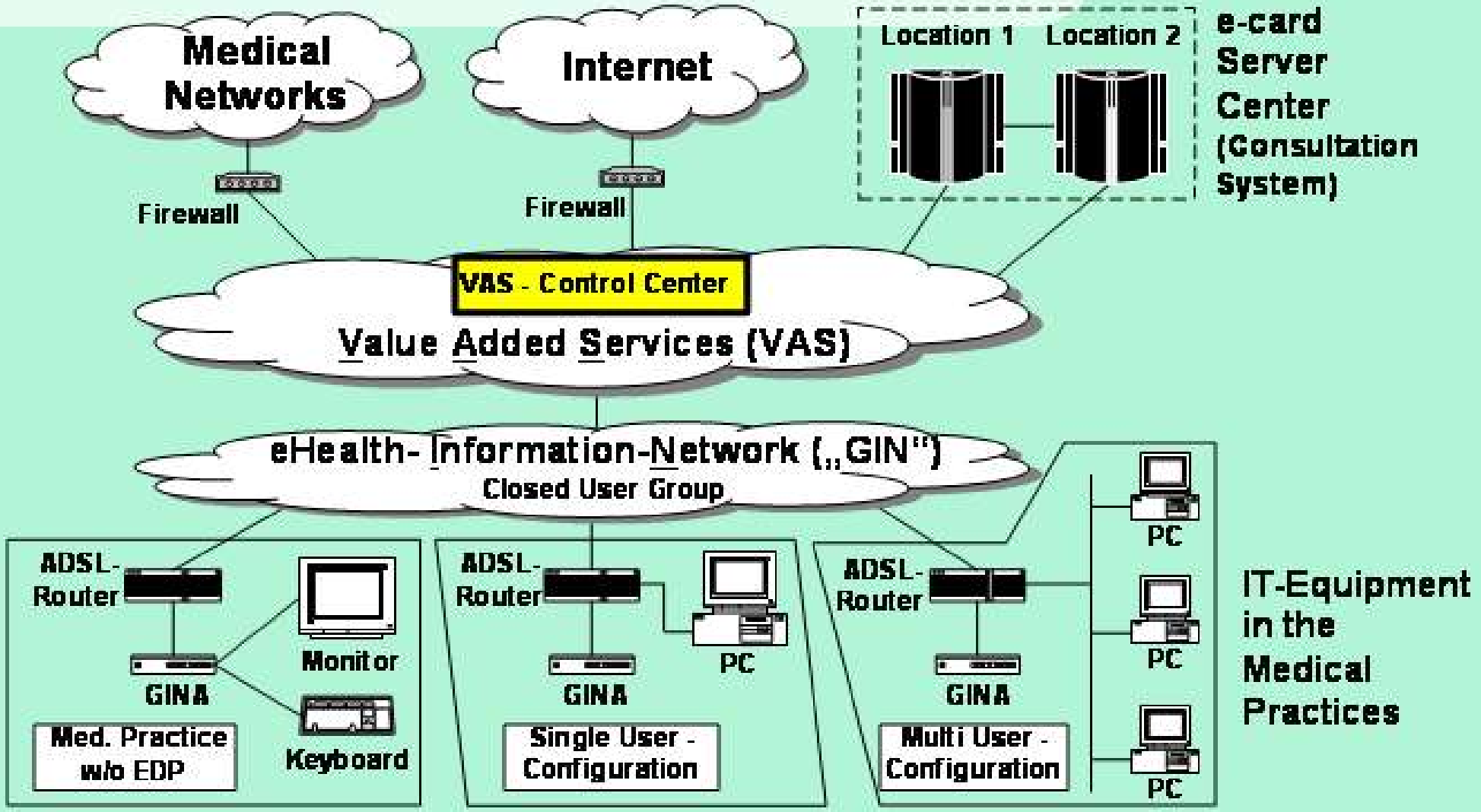
- = **XML Data stucture** which comprises
  - Base Identification Number
  - public keys
  - frequently used personal data
  - (name, date of birth).

  signed by „**Base Identification Number Register Council**".
- Stored on the Citizen's Card
  - under Control of the Citizen
- **Confirms the link** between
  - **identification data** (Base Identification Number)
  - **authentification data** (Signature Creation / Verification Data)

```
<saml:SubjectConfirmationData>
  <pr:Person
si:type="pr:PhysicalP
-   <pr:Identification>
      <pr:Value>4dwsdW...Q==</pr:
V
      <pr:Type>http://reference.e
-g
    </pr:Identification>
- <pr:Name>
    <pr:GivenName>Herbert</pr:Giv
en
    <pr:FamilyName>Leitold</pr:Fa
mi
  </pr:Name>
  <pr:DateOfBirth>1965-08-12</pr
...
```

Overview: e-card Network

ecard



SVC

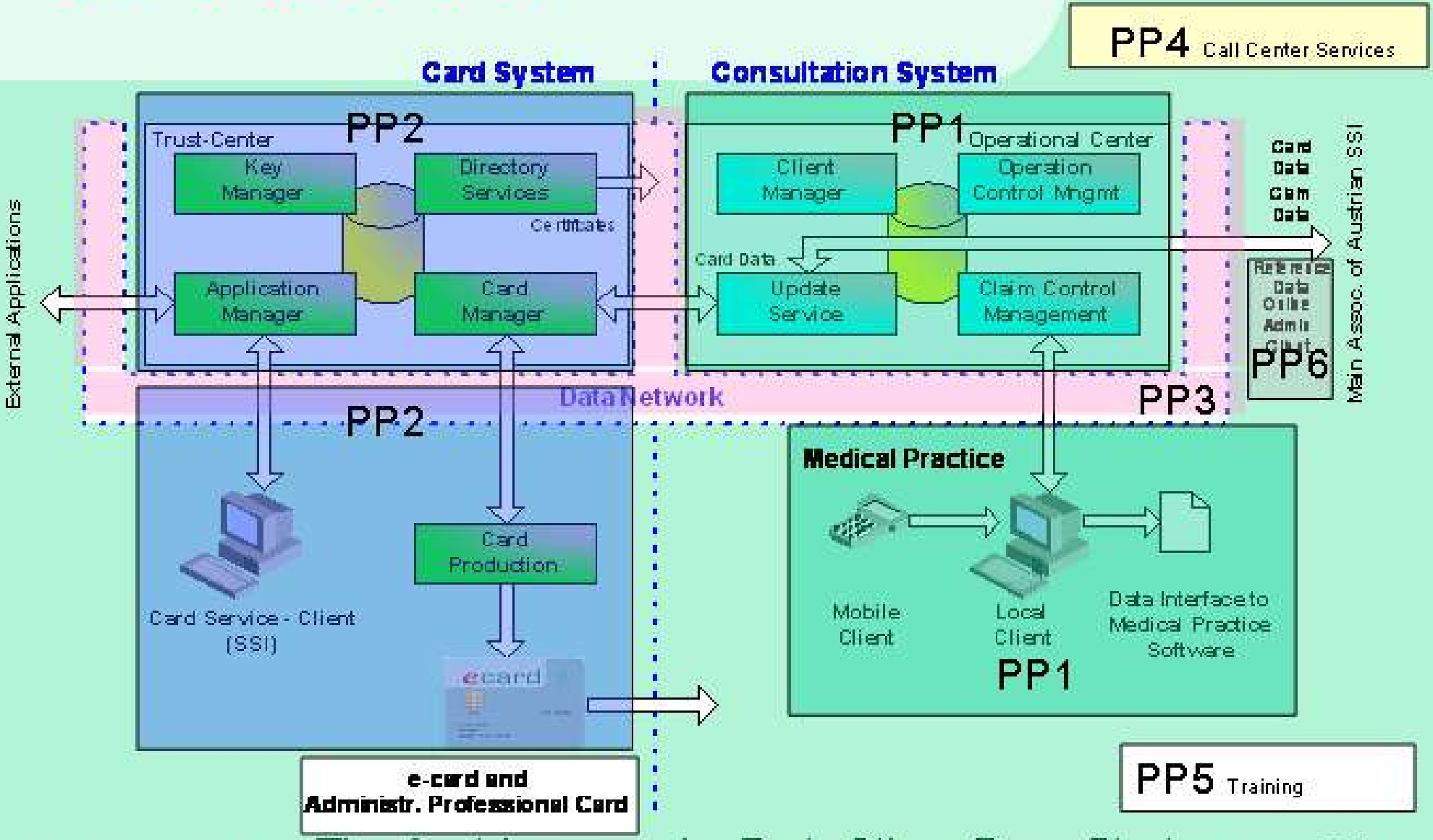
System Division into Partial Projects

ecard

- **PP 0: System Integration**
- **PP 1: Consultation System**
  („Operational Server Centre and Terminal-Software")
- **PP 2: Card System**
  (Health Insurance Smart Card-System and Trust Center-Functions)
- **PP 3: Communications Services**
  (Data Networks, including Rollout of corresponding IT-components)
- **PP 4: Call Center**
  (Customer Services of the Social Security Institutions)
- **PP 5: Training**
  (Training of Personnel: User Interface in the Medical Practice)
- **PP 6: Administration Client of Social Security Institutions**

PP1 to PP6

ecard



Status of the Project

ecard

Partial Project	Name of Partial Projects	Contract Award	Contractor / Organization (Subcontractor)
PP1	**Consultation System** (Operational Server Centre and Terminal-Software)	03.01.2004	Siemens Business Services GmbH & Co, (IBM-Österreich GmbH, Telekom Austria AG, Scientific Games International GmbH)
PP2	**Card System** (Health Insurance SmartCard-System and Trust Center – Functions)	09.04.2004	Giesecke & Devrient GmbH (Deutsche Post Sign Trust GmbH, Bell ID B.V., Bundesrechenzentrum GmbH)
PP3	**Communications Services** (Data Networks, incl. Rollout of corresponding IT-components)		Telecom Provider
PP4	**Call Center**	18.08.2004	Competence Call Center AG
PP5	**Training** (for Personnel dealing with User Interface in Medical Practices)	CRQ 07/2004	Performed by PP1
PP6	**Administrative Client** (of the Social Security Institutions)	03/2004	Main Association of Austrian Social Security Institutions

SVC

Strategic Projects:
Integration of further Partners

ecard

In the fields of eHealth and Social Security, e.g.

Hospitals
(out-patient clinics)

Pharmacies
(Electronic Prescription)

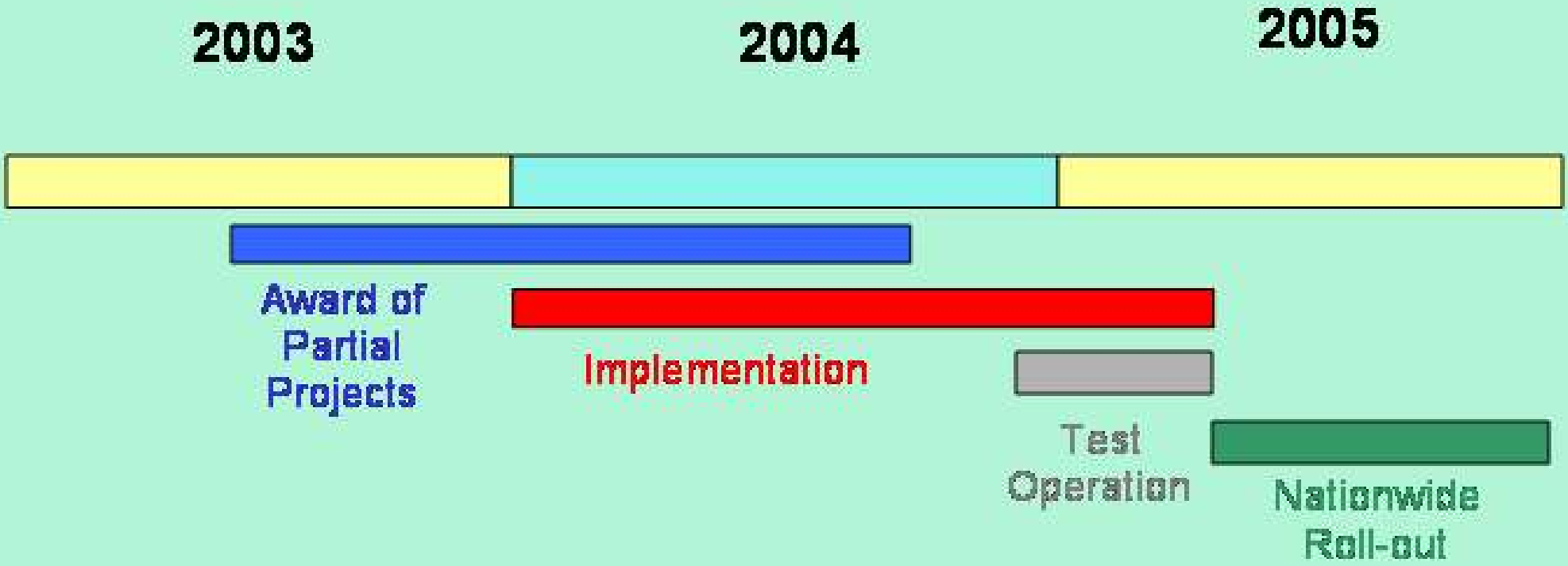
Medical Data Bases
(Secure access to diagnostic findings)

Employers
(Insurance Registration & Deregistration Process)

...and access to (new) eGovernment Applications

Time Schedule

ecard



Vision of e-card usage

ecard

- **Social Security**
  Replacement of all paper based health insurance certificates
- **eHealth**
  Keycard for secure handling of medical transactions
  (basic token for eHealth Telematics)
- **E-Government**
  Signature and Encryption Card for all fields of application with corresponding requirements
- **eApplications for Third Parties**
  By use of the Infobox-Concept for Keys and Authorizations
- **eCommerce**
  Signature and Encryption Card with cooperating Partners.

ecard


The SVC-project team
thanks for your
attention !
Contact: heinz.otter@chipkarte.at
www.chipkarte.at