ecard

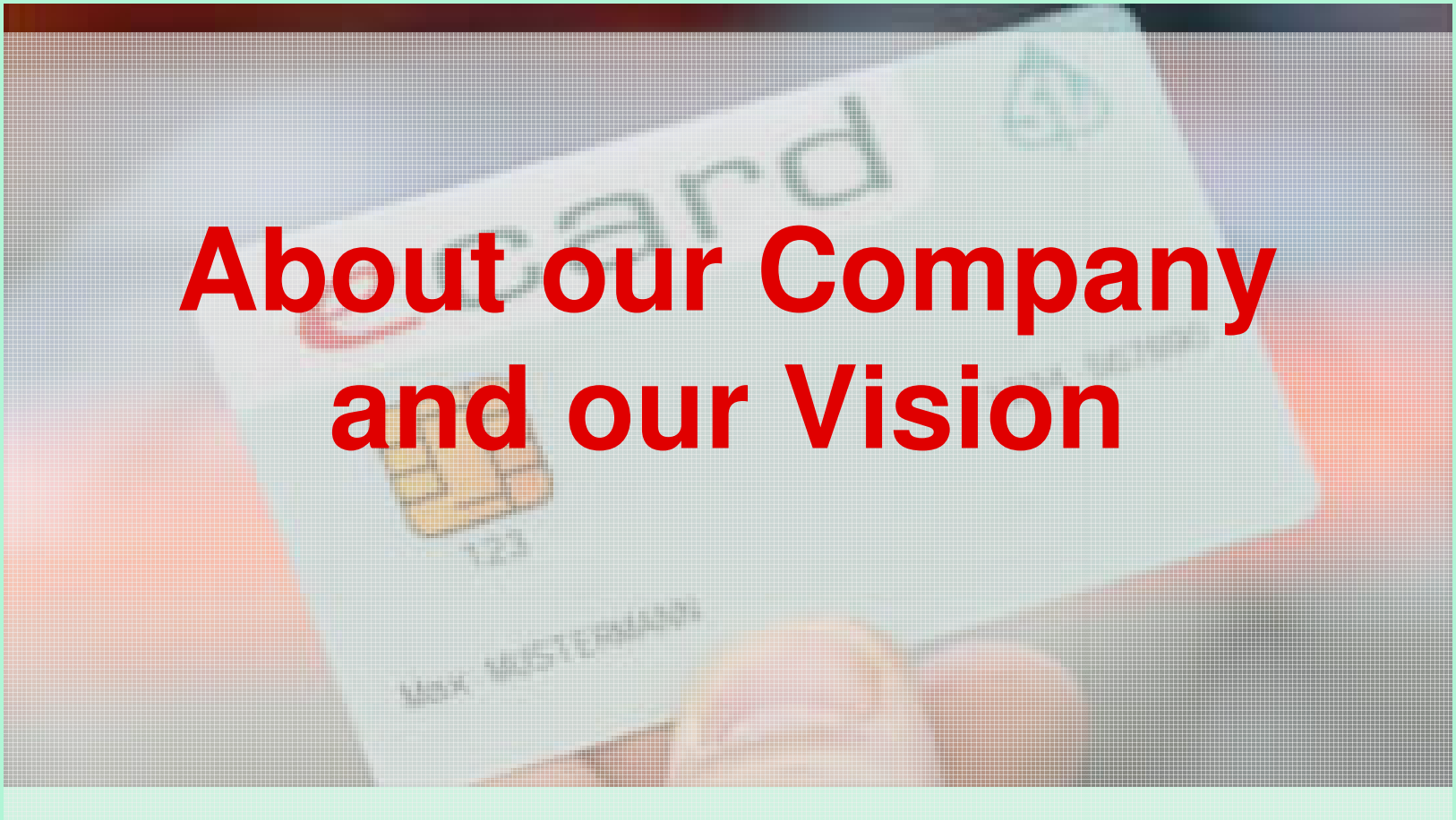
Status and Vision of the Austrian e-card

Dipl.-Ing. Heinz Otter

eHealth 2005, International Day, Munich, 21.04.2005

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

Chapter 1



SVC:
‚Chipcard Systems Establishing and Operating Company Ltd.‘

- Our „SVC“ is responsible for the establishment of the project and is in charge of operating the system
- founded February 24th, 2001
- 100% owned by the „Main Association of Austrian Social Security Institutions“

The „SVC - Company“

- The **SVC** is **system integrator**
  Implements the „**E**lectronic **A**dministration **S**ystem“ **(ELSY)** on behalf of the „**M**ain **A**ssociation of Austrian **S**ocial **S**ecurity **I**nstitutions“ (**MASSI**)
- 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**.
- First Step:
  Substitution of the health insurance vouchers by a **smart card.**

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

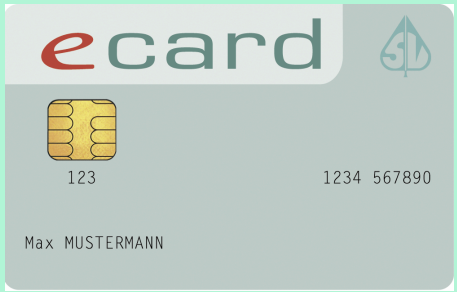
Specific Vision:
e-card applications in the fields „Social Security and eHealth“

Hospitals

Out-patient Clinics

Medical Practices

Pharmacies



Ambulance Services

Dentists

Social Security Services

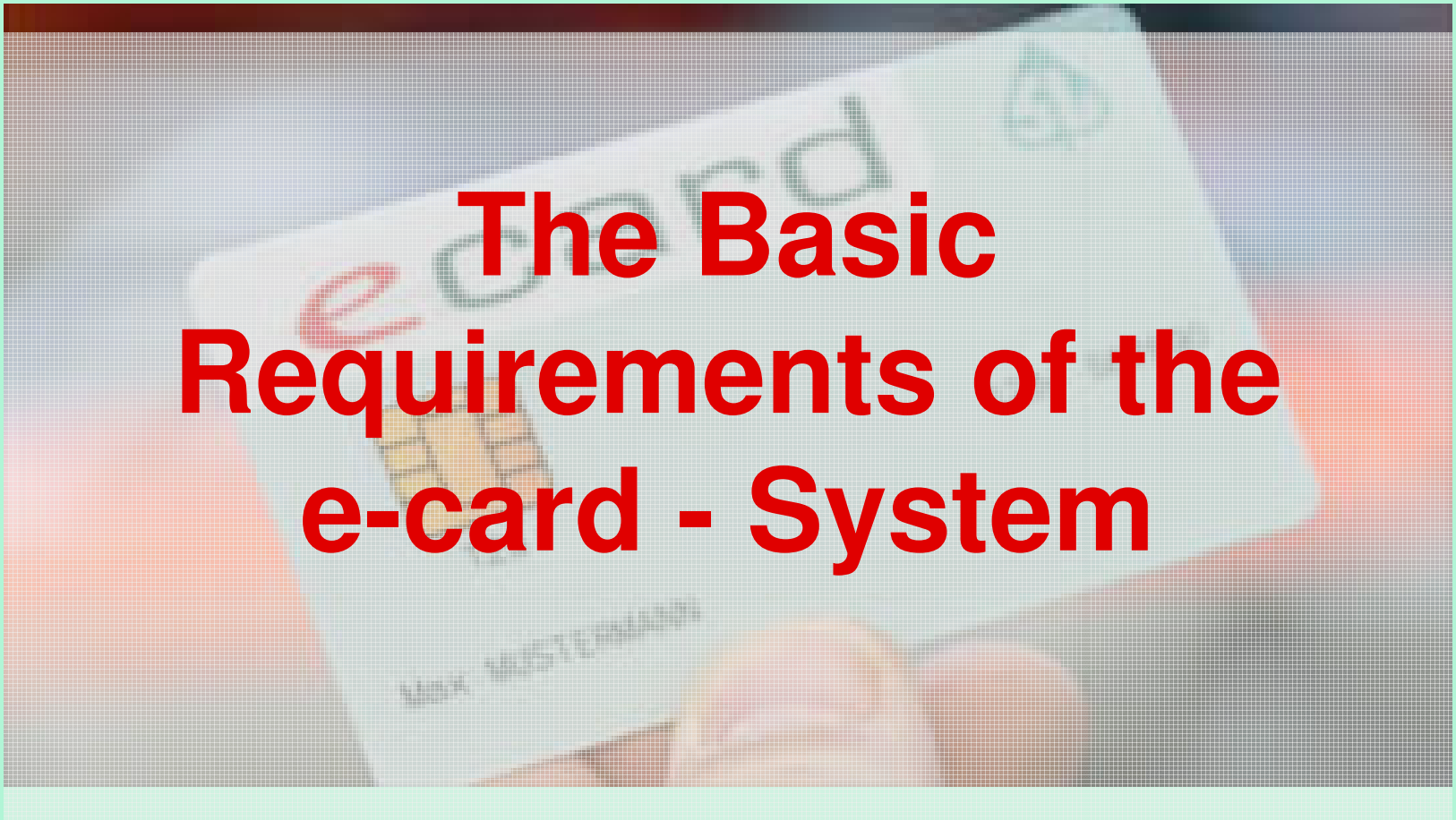
Keycard for „eSocSec-Portal“ (= eGov-Appl.)

Extended Vision: e-card‘s Functionalities & Applications

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 access protected storage files („Infoboxes“) for Keys and Authorization
- **eCommerce**
  Signature and Encryption Card with cooperating Partners.

Chapter 2



The Keycard-Principle

ecard

- Physically the **e-card** corresponds to an i**ntelligent 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 **access authorization** to applications.

Requirements to the Compound System

ecard

Government (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**“:
  Interfaces to local IT-Infrastructure and data networks will be standardized and supported by this „Adapter 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 available 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

- **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 **counterfeiteproof**
- **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.**

Chapter 3

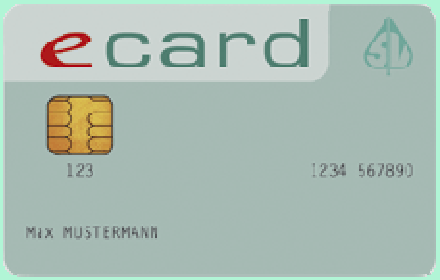
e-card's Initial Application: "Replacement of Health Insurance Vouchers"

Initial Application: „Replacement of all Health Insurance Vouchers in Use“

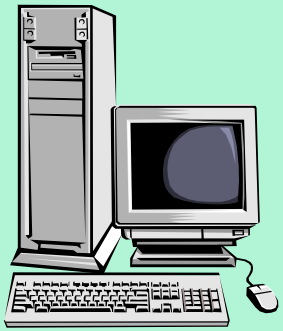
ecard

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

Key-Data



Supply **8 million** e-cards for **insurance**



Integration of about **12.000 contractual partners**
- Software clients for medical practices
- chipcard readers
- via **„Medical Practice Unit (MPU)“**

SVC

Present Process: „Consultation with a Doctor“

ecard

Employer

Issue of health insurance vouchers

Employee

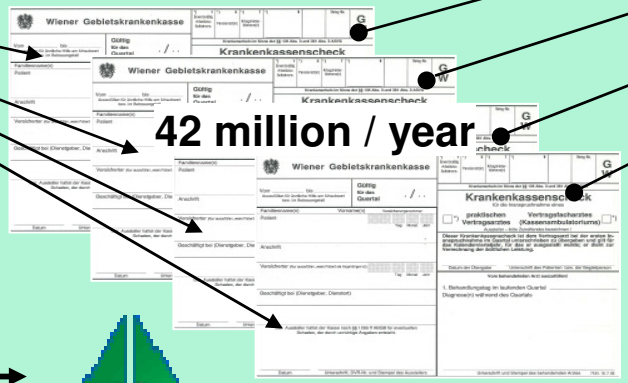
Physician

(1)

Insurance status:
Registration &
Deregistration process

Computer System(s)
Social Security Institutions

(2)



42 million / year

(3)

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

(4)

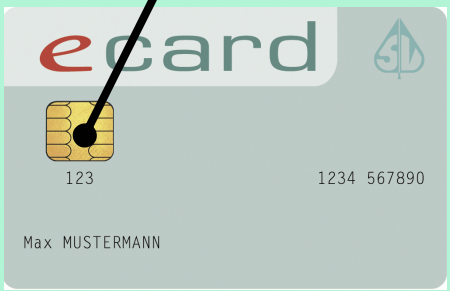
....**Accounting**

SVC

Future Process: „Consultation with a Doctor“

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

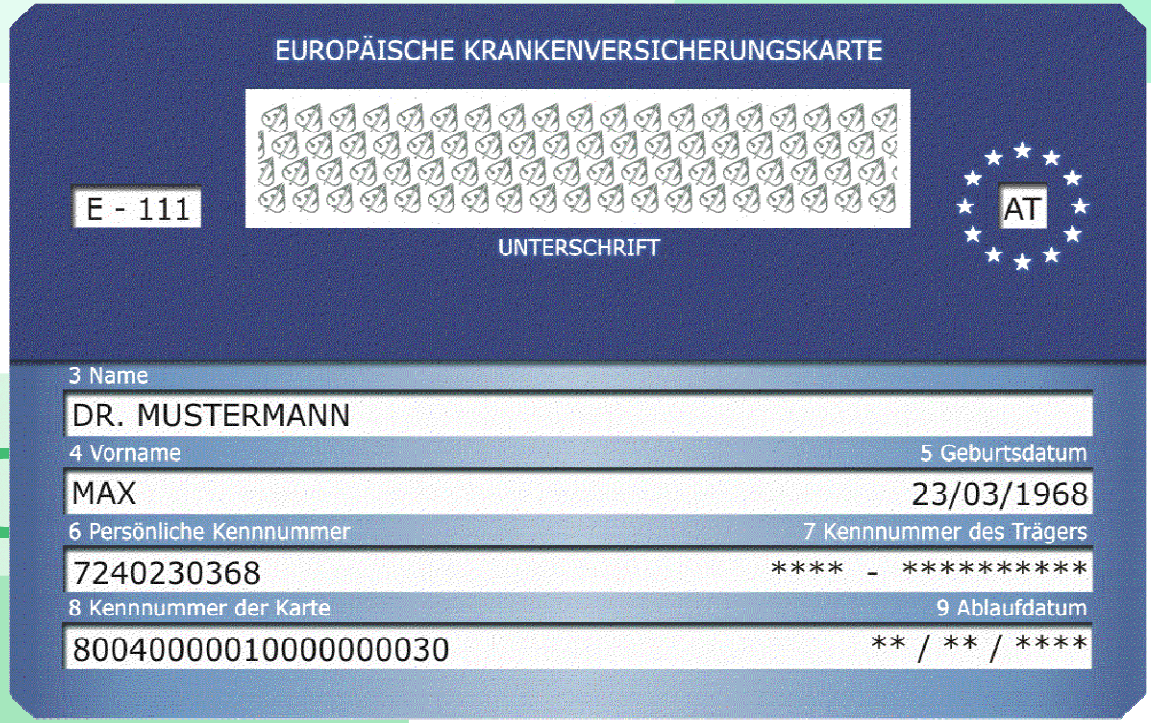
Online Check of Claim (SV-Signature protected)

„Consultation Server Center“ for e-cards

SVC

Layout of the e-card

ecard



ecard

123

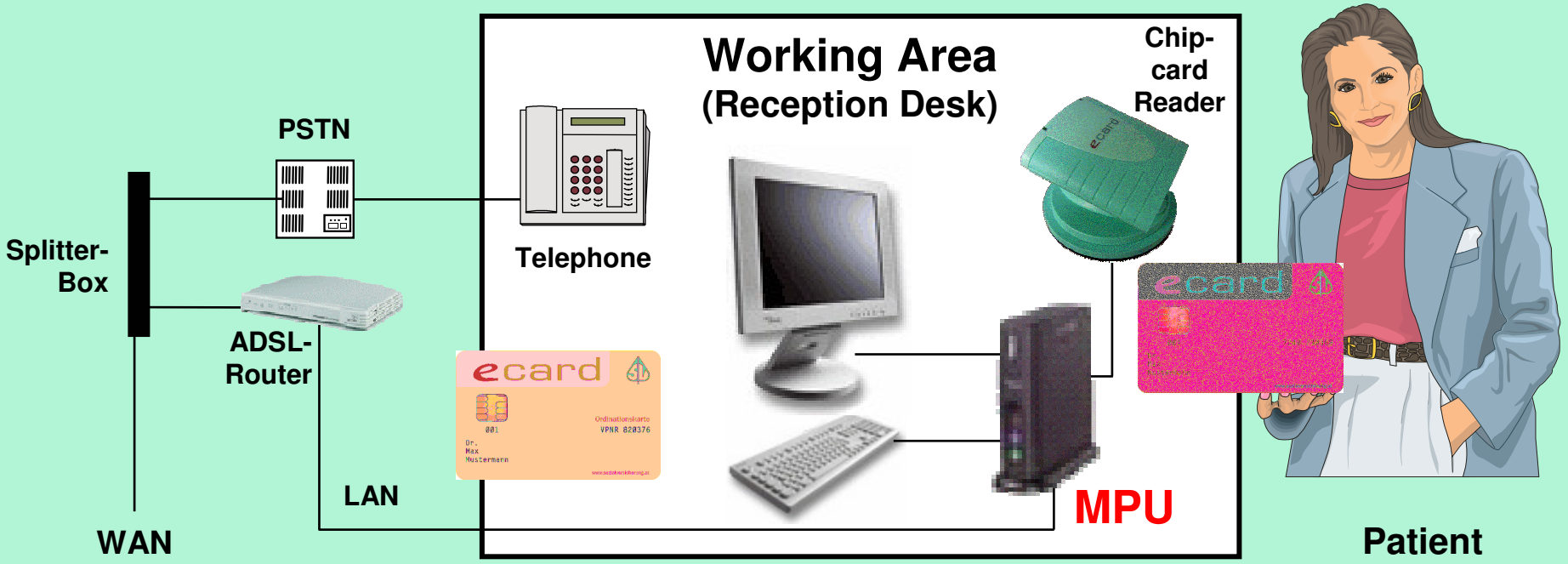
1234 567890

Dr.
Max
Mustermann

www.sozialversicherung.at, Serviceline 050124 33 11

Doctor‘s IT Equipment: Medical Practice Unit (MPU) is Core of a Single Workstation

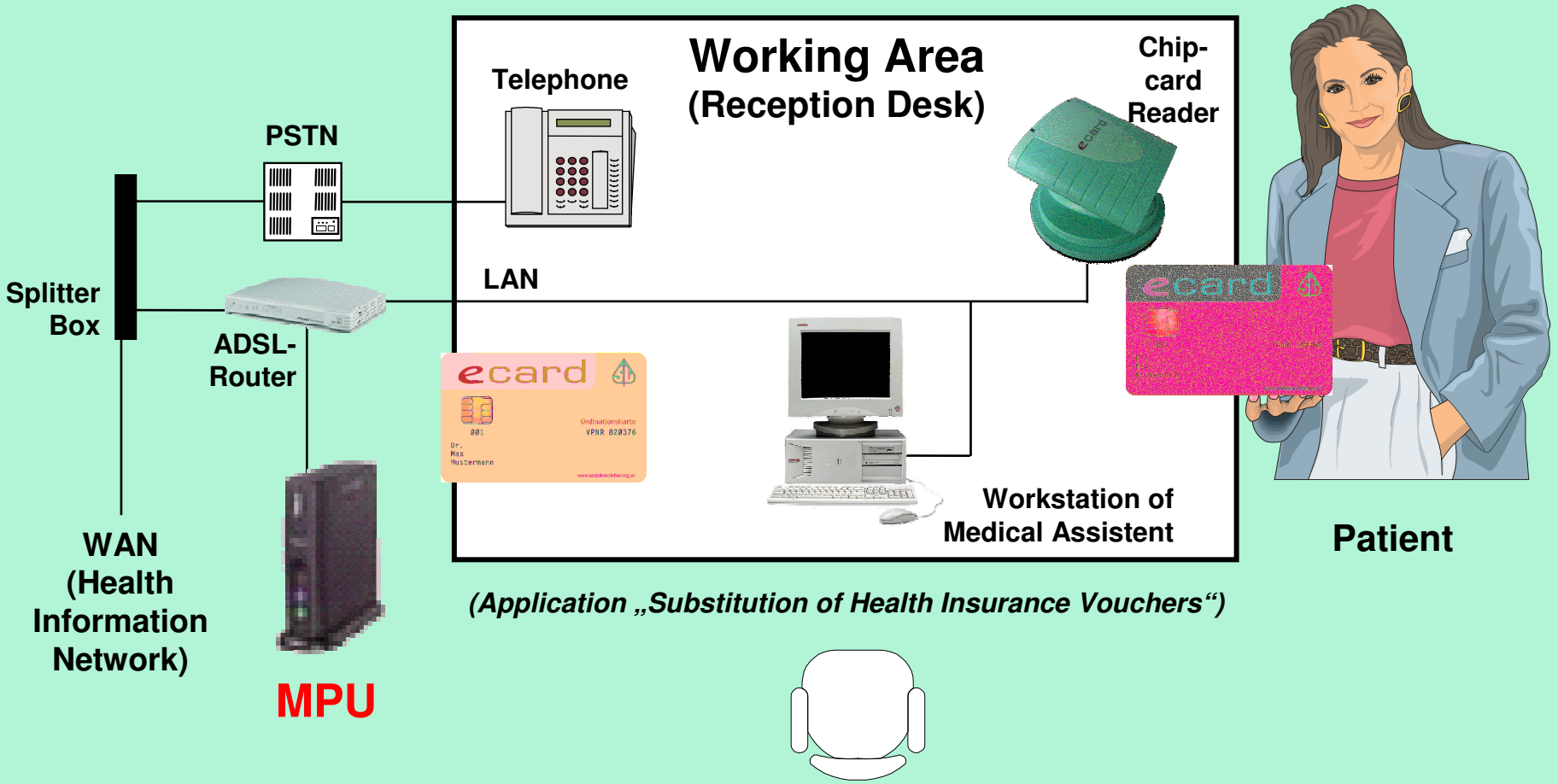
ecard



(Application „Substitution of Health Insurance Vouchers“)

Doctor‘s IT Equipment: Medical Practice Unit (MPU) & Single Workstation with LAN

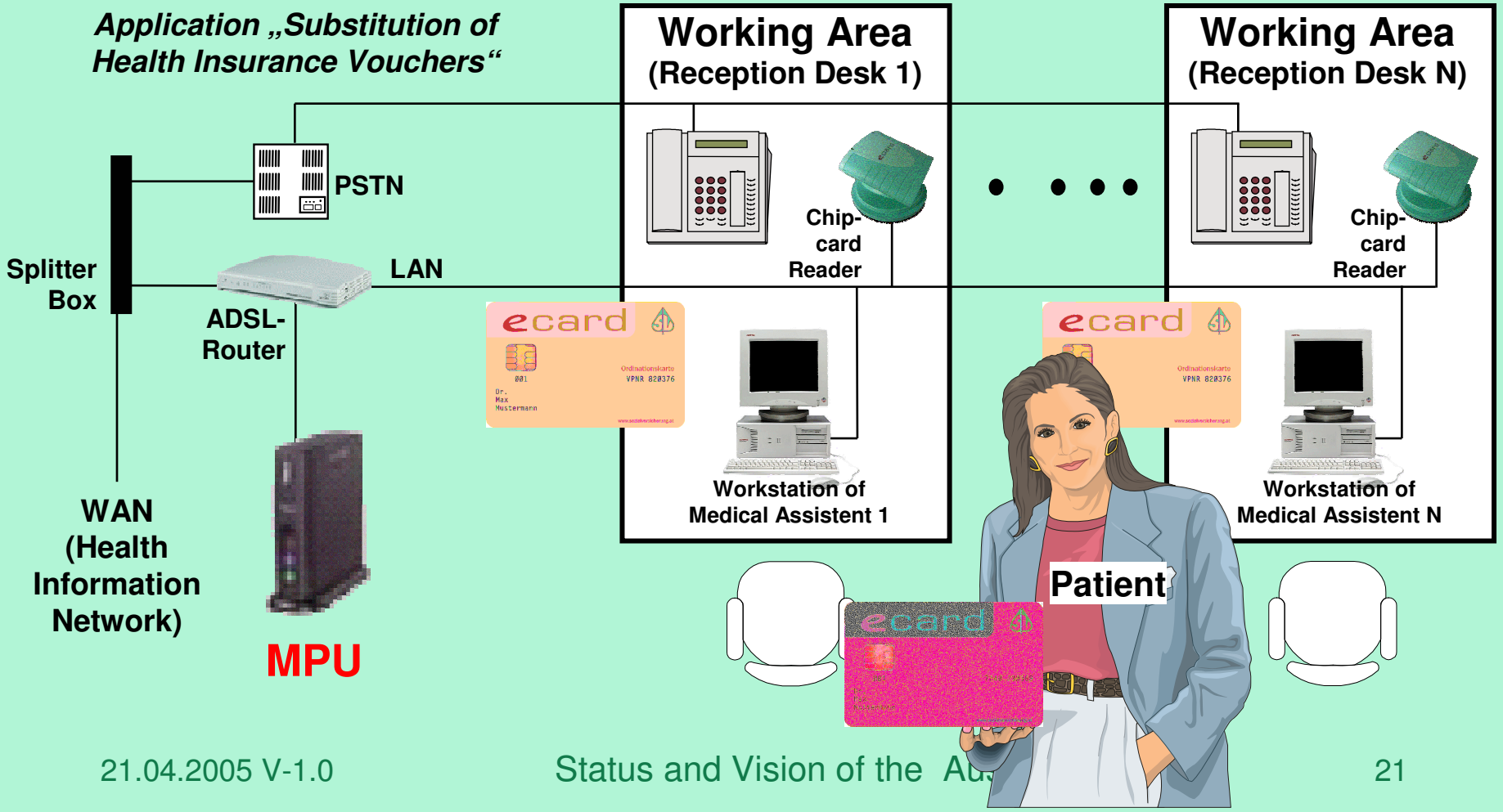
ecard



(Application „Substitution of Health Insurance Vouchers“)

Doctor‘s IT Equipment: Medical Practice Unit (MPU) & Multi User Configuration (LAN)

ecard



Advantages of the e-card

Insured

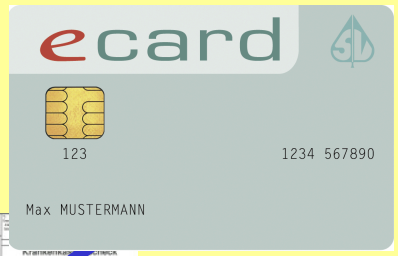
- **Protection of privacy**
- **Easier access to medical help**

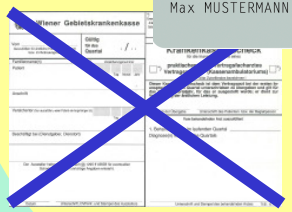
Physicians

- **Efficient use of EDP**
- **Minor administration expenses**

Employer

- **No issue of health insurance vouchers**

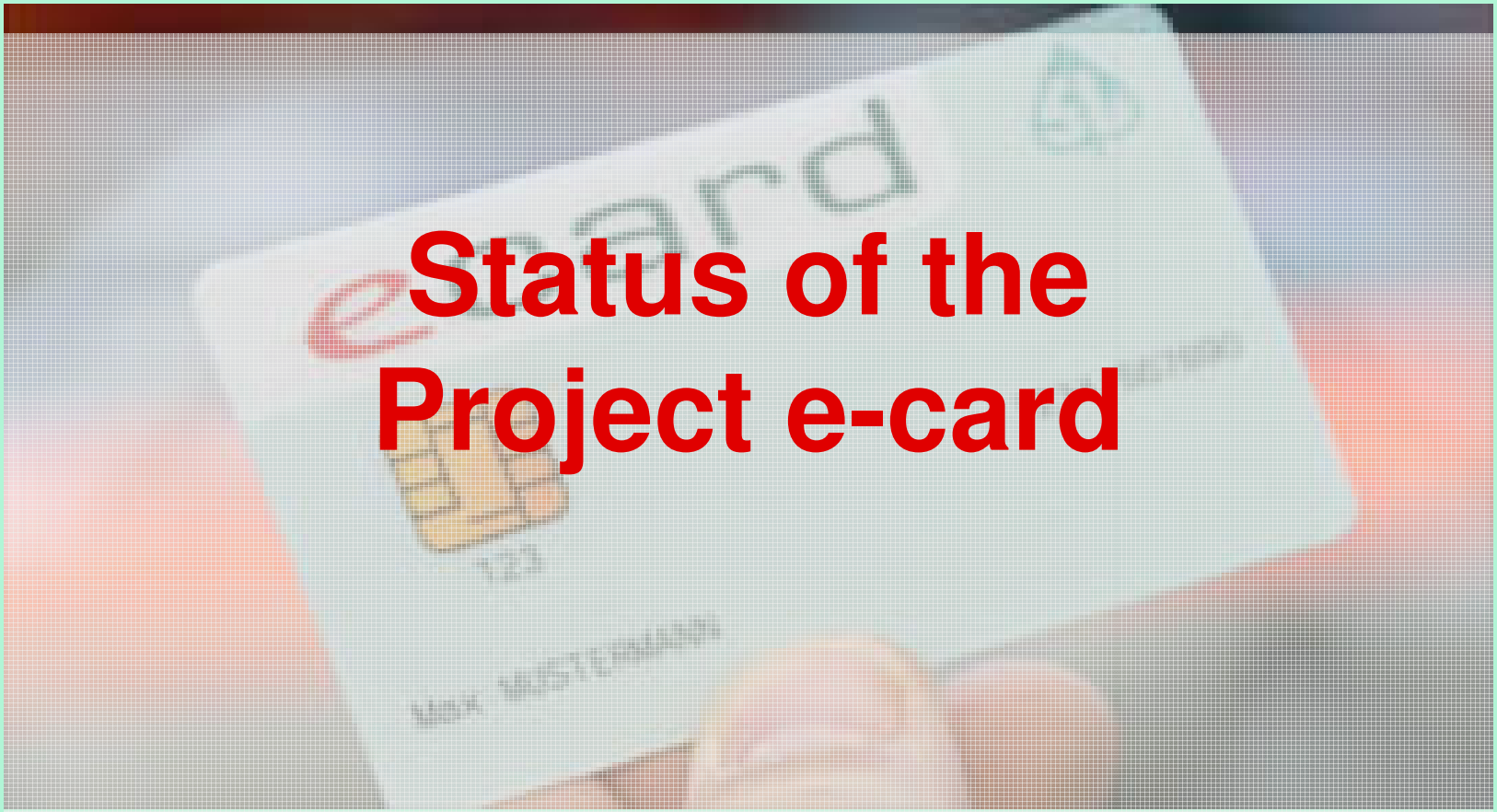




Social Security

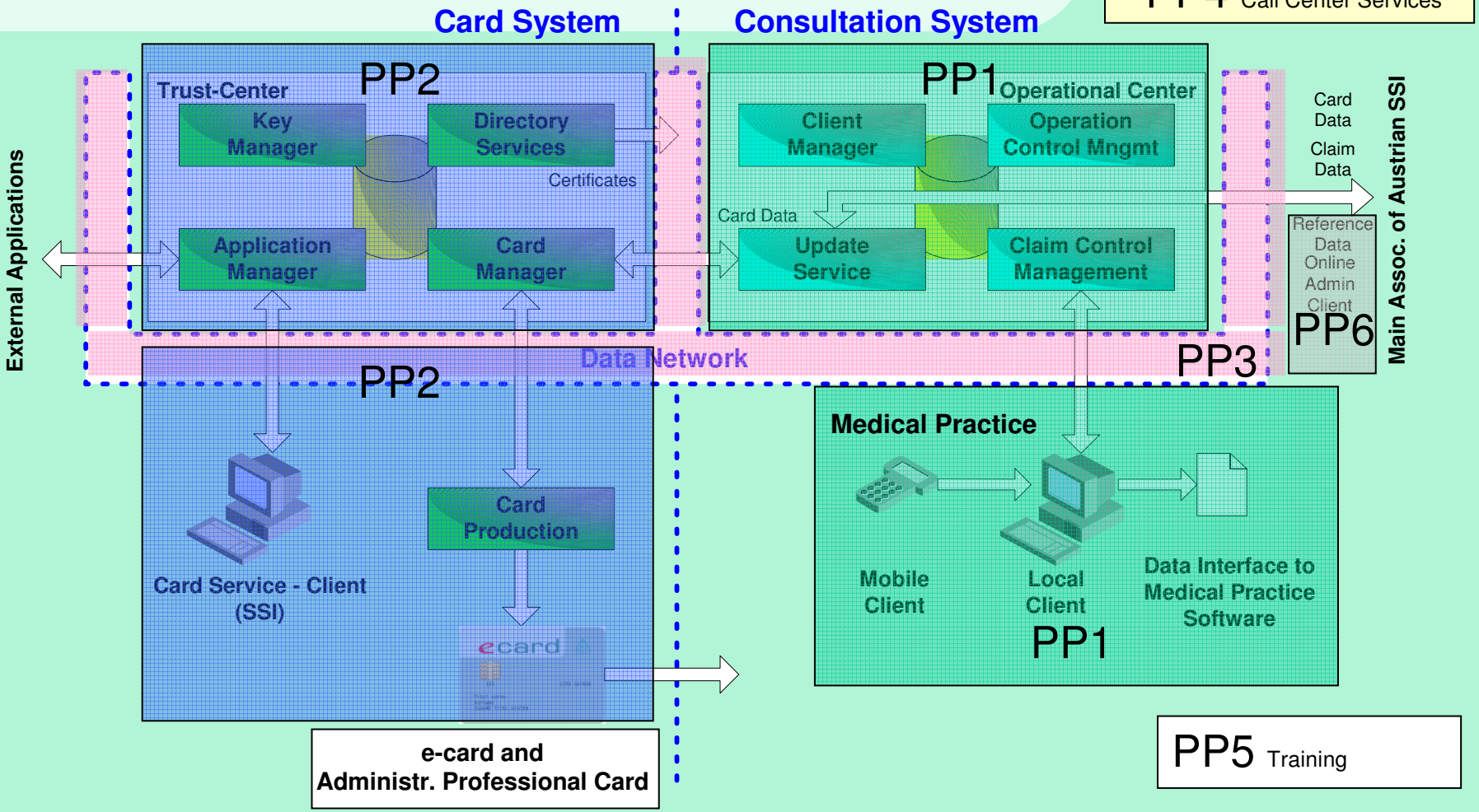
- **Secure claim check**
- **Minor administration expenses**

Chapter 4



Status of the Project e-card

Partial Projects PP1 to PP6



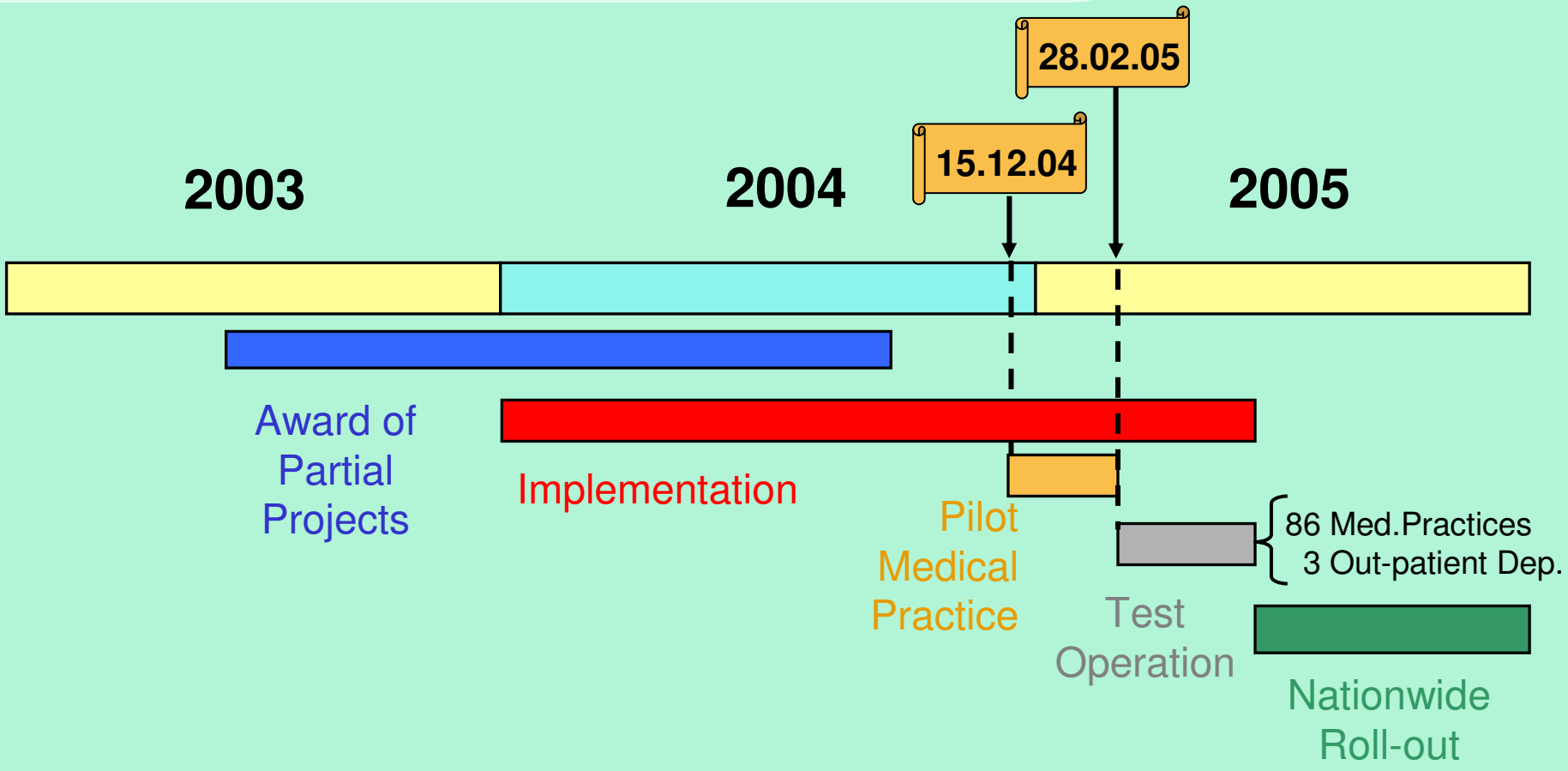
Status of the Project

ecard

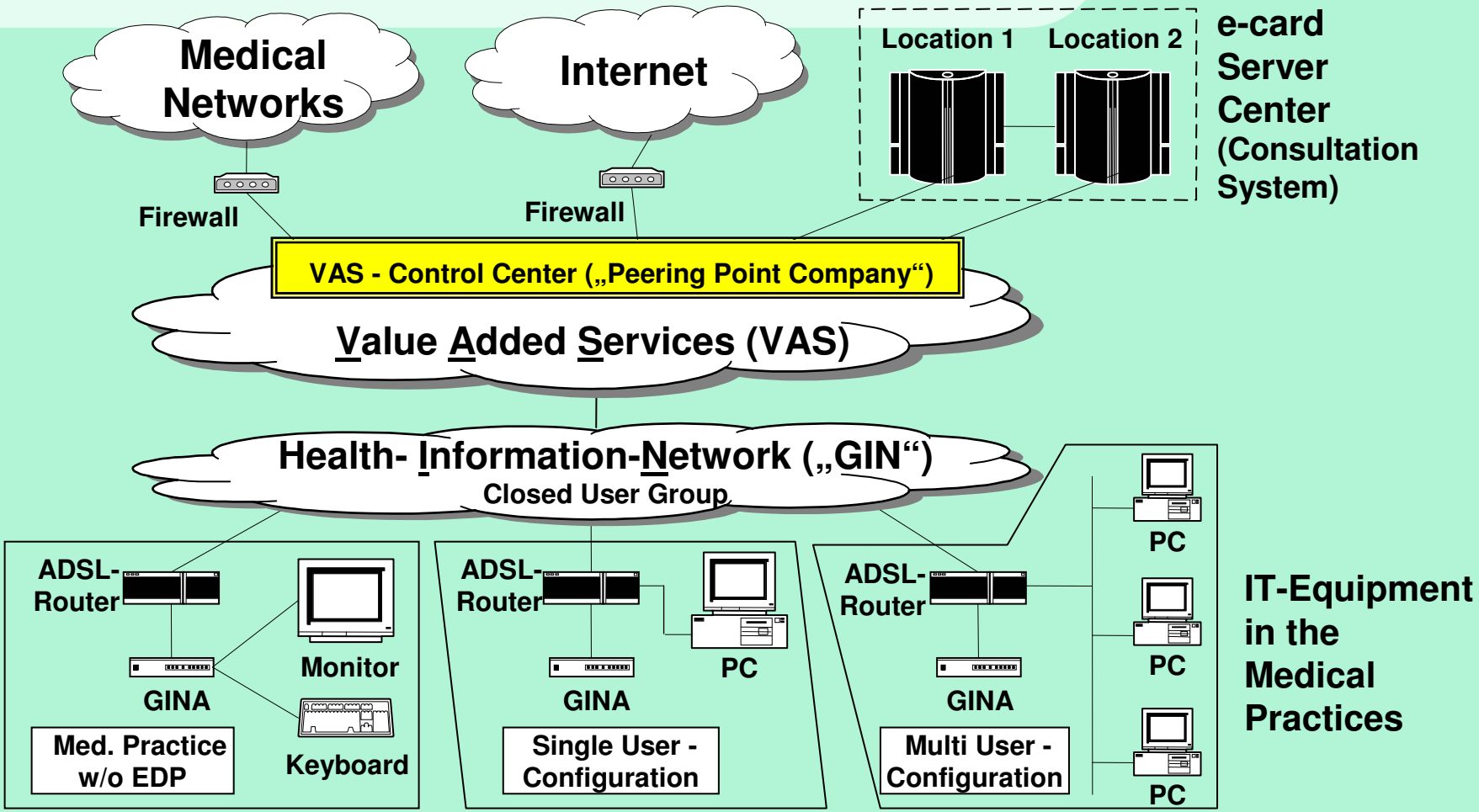
Partial Project	Name of Partial Projects	Contract Award	Contractor / Organization (Subcontractor)
PP1	**Consultation System** (Operational Server Centre and Terminal-Software)	03.01.2004	**Siemens Business Services GmbH & Co,** (IBM-Österreich GmbH, Telekom Austria AG, Scientific Games International 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 Providers**
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

Time Schedule e-card: Replacement of Health Insurance Vouchers



Overview: e-card Network



SVC

e-card Networking combines:

➔ Multiapplicative Frame &

➔ Value Added Services

- **Multiapplicative Frame of e-card System**
  - **Health-Information-Network** (GIN)
  - IT of Medical Practice ←→ e-card–Serversystem
  - Closed User Group (ADSL-Network)
- **Value Added Services for Physicians**
  - **VAS-Network** with **VAS-Control Center („Peering Point“)**
  - IT of Medical Practice ←→ Internet, e.g. for eGovernment
  - IT of Medical Practice ←→ Medical Networks for ...

    Value Added Services (e.g. Transmission of Findings)
- **VAS-Control Center controls Kind of Transaction**
  - e-card applications / Internet-Service / Medical Networks
  - Priorities / Throughput

SVC

Experiences with respect to Acceptance

ecard

- **Testoperation: 28.02. until 30.05.2005**
  Scope: 104.000 e-cards, 86 medical practices (plus 56 expected), 3 out-patient departments
- **Satisfied endusers in medical practices**
  System runs stable with expected performance. Man-machine-interface replaces manual administrative processes effectively - but is still target of optimization
- **Satisfied cardholders / patients**
  Simple access to medical help combined with more privacy derive remarkable advantages for everybody

Chapter 5

Managing Accessibility: e-card's role in the Austrian eGovernment - Strategy

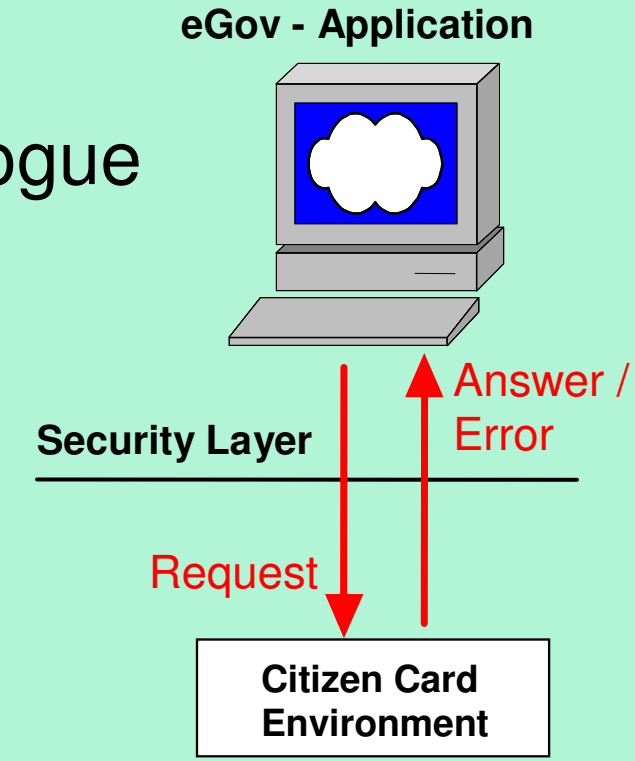
e-card provides Core Features for the Austrian eGov-Strategy

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“, a software provided by the Austrian Federal Government, available for everybody via download: www.cio.gv.at/identity/bku

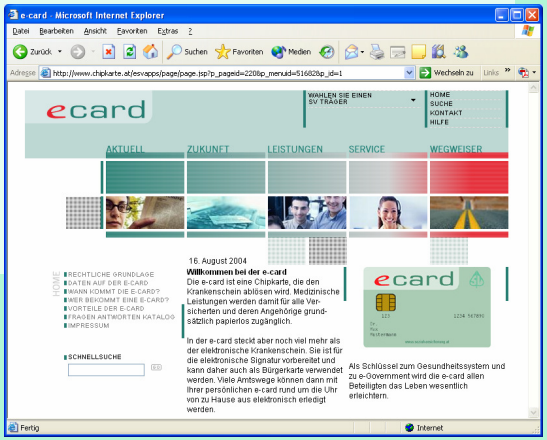
eGov–Strategy: Protocol Structure and Citizen Card - Environment

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



SVC

eGov–Strategy: Security Layer



ecard

eGov - Application

Security Layer

Citizen Card Environment

PIN Input

Trusted Viewer

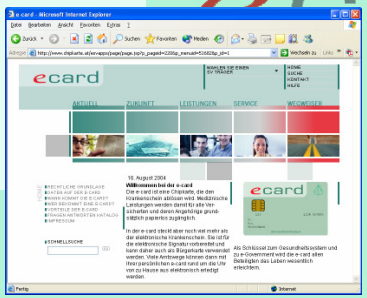
Hash-Function

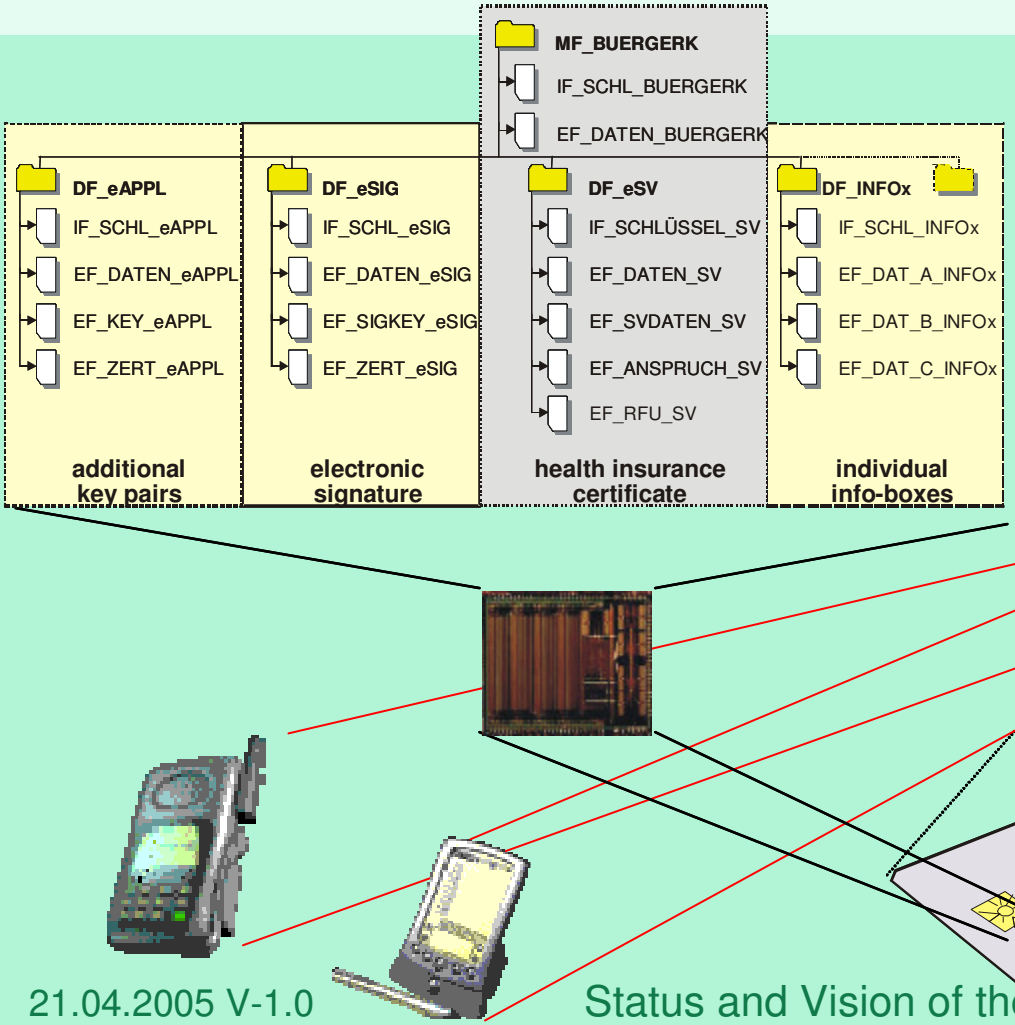
Card Interface (e.g. PKCS#11)

Add on Memory

SVC

eGov–Strategy: Technology Independence





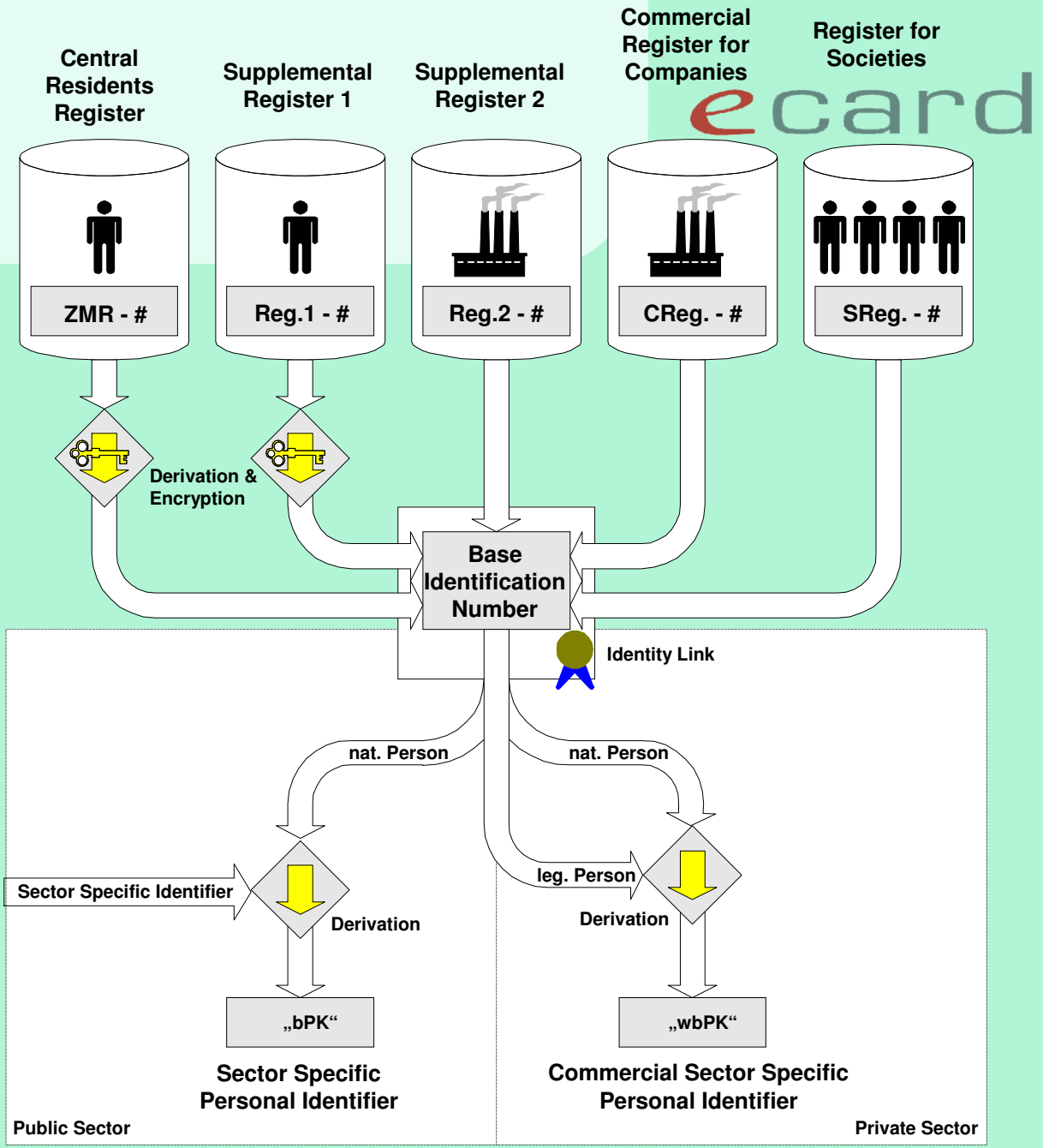
eGov–Strategy: „Identity Link Parameters“

- **„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

eGov–Strategy

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



21.04.2005 V-1.0

eGov–Strategy
Identity Link (e.g. in XML)

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:Given
    <pr:FamilyName>Leitold</pr:Fami
  </pr:Name>
  <pr:DateOfBirth>1965-08-12</pr
...
```

SVC

Electronic Signatures of the e-card

3 signature applications on card:

- **Administrative electronic signature** (according to VW-SigV)
  for eGovernment and eCommerce applications
- **Advanced electronic signature**
  for general applications, where no secure signature is required

„eGov“

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

„eSocSec“

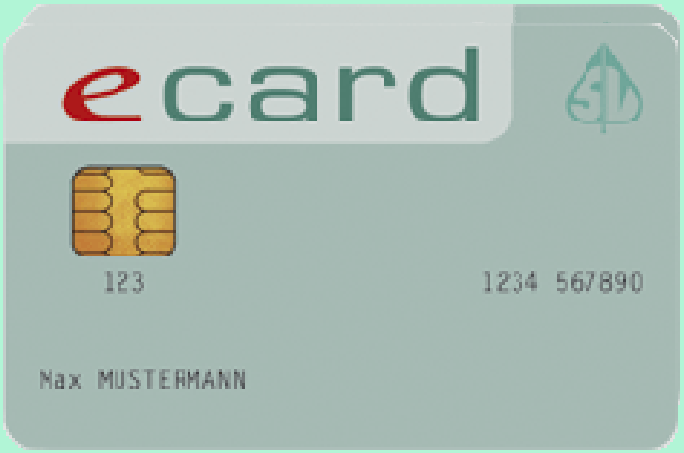
Chapter 6

Outlook: Enlargement of the e-card - Project

EHIC: EU Health Insurance Card - Steps towards EU-Interoperability

Replacemant of Voucher „E-111“ via European Health Insurance Card (EHIC)

Implementation of the EHIC on/in the e-card as well as substitution of the international health insurance voucher E-111 within the scope of the Project Netc@rds



SVC

Strategic Projects:
Integration of further Partners

ecard

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

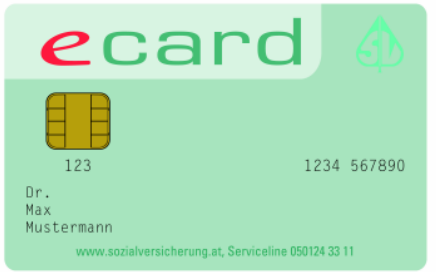
Hospitals
(out-patient clinics)

Pharmacies
(Electronic Prescription)

Medical Data Bases
(Secure access to diagnostic findings)

Employers
(Insurance Registration & Deregistration Process)

...and access to (new) eGovernment Applications



ecard

Thank you very much for your attention!

contact: heinz.otter@chipkarte.at
www.chipkarte.at