advanced aspects of IT infrastructure in healthcare (The Austrian e-card System)

Linz, Oktober 2012

Agenda

- The Austrian e-card System - System Overview
- Requirements
- HA (high availability) datacenter and concepts
- Stages and staging
- Network, network services, monitoring and SLA monitoring
- Callcenter, Operating & Ticketing
- Support of ISVs
- SW Distribution
- HW-Infrastructure on health providers site (GINA, LAN-CCR, Router)
- Pseudonymisation / STS
- e-card infrastructure in ELGA
- What's next ?

SVC

Social Insurance Institutions

Electronic Transmission of Medical Findings

Value Added Services (VAS)

Preoperative Questionnaire

e-Health Portal

Online Backup

e-card System/ Data Center

GIN / eHI-Net
Health Information Network
eHealth Interconnection Network

VAS Access

GIN Access

GIN Access

Pharmacies

Physicians

eHI-Net

eHI-Net

Hospital Associations

Hospitals

eHealth Applications

eHealth Applications

3

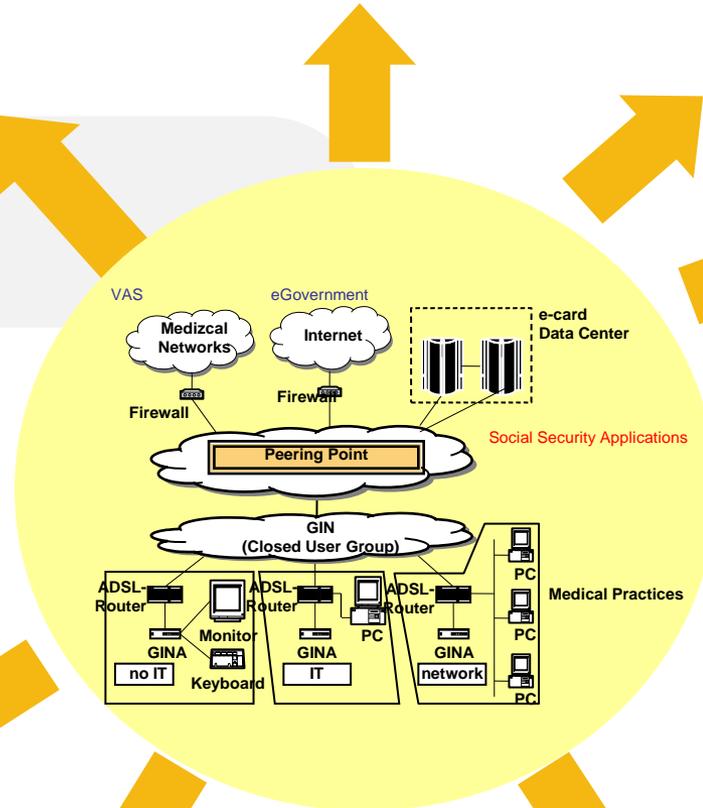# Applications, services and facilities

Applications

- Electronic Check of Entitlement
- Medication Approval Service
- Social Security Query Service
- Preventive Medical Checkup
- Electronic Temporary Disability Report
- Disease Management Programmes

e-card System Operation

Infrastructure ready for eHealth

Trust Center and Card Service Portal

Citizen Cards

- >67.000 Signatures

Call Center

- Hotline for Healthcare Providers
- Hotline for Insured

eMedication

- ELGA – eMedication
- Pilot in 3 Regions (Vienna, Upper Austria, Tirol)

Care Facilities

Hospitals

VAS
Medizcal Networks
eGovernment
Internet
e-card Data Center
Firewall
Firewall
Peering Point
Social Security Applications
GIN (Closed User Group)
ADSL-Router
ADSL-Router
ADSL-Router
Monitor
PC
PC
Medical Practices
GINA no IT
Keyboard
GINA IT
GINA network
PC
PC

Facts & Figures

- e-cards (active)   ~ 8.900.000
- new e-cards (births, changes…)   ~ 850.000 p.a.
- Health Care Providers connected   ~ 11.000
- Pharmacies   ~ 120
- Hospitals   ~ 140
- Care Facilities   ~ 15

- e-card Consultations
  – since March 2005   ~ 667.763.920
  – average contacts per day   ~ 500.000
  – all time high (Dec. 14th, 2009)   629.150

- Citizen Cards   ~ 67.000

Facts & Figures (contd.)

- SVC: ~ 100 employees
  - 42 in development

- Development
  - 25 developers and analysts
  - 9 system testers
  - 8 plattform engineers (App- and DB-Server, build&deployment, GINA, LAN-CCR)

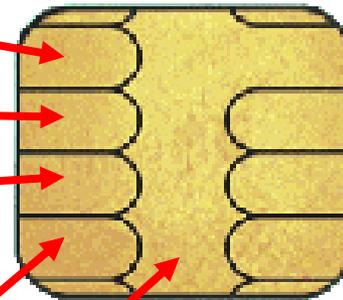# The Austrian e-card

Front Side = **e-card**   Reverse Side = **EHIC**
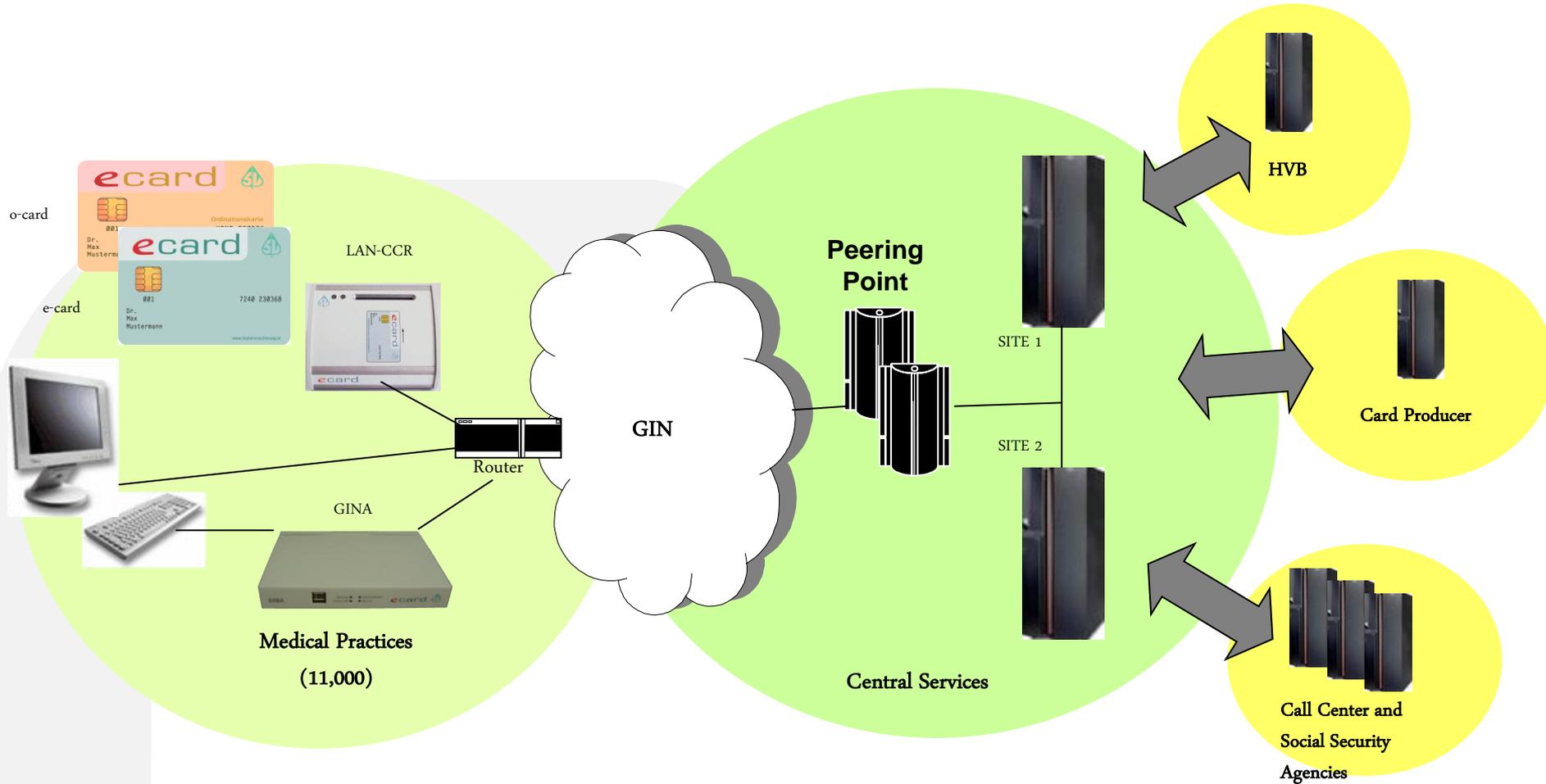
Data in the Chip

- All eye readable data

- Gender

- Different cryptographic keys

Optional:

  - Digital certificates (citizen card)

- Not in use:

  - User group identification

  - Storage for future use

System Overview

o-card

e-card

LAN-CCR

GINA

Router

Medical Practices

(11,000)

GIN

Peering
Point

SITE 1

SITE 2

Central Services

HVB

Card Producer

Call Center and
Social Security
Agencies

Requirements

- 2 factor authentication for the MP
- Authentication solution of the patients must also be usable as citizen card (for eGovernment services)

- Guaranteed response times and bandwidth
- Network only reachable for entitled MPs (avoid using stolen MP identities over the web)
- Network not reachable from the internet (avoid denial of service and other security attacks from the web)
- Appropriate border protection

- End-to-End encryption for certain services

Requirements (contd.)

- Standalone functionality (for MPs without any computer, to spare them IT investment)
- Minimal footprint in MP's IT infrastructure (No need to install software or drivers on MP's site)

- Offline functionality for critical services (consultation) in case of network or central service outages

- Multi host chip card reader, to support more than one workplace with one chip card reader
- Hide complexity of handling smartcards from software vendors (Access of the cards and activation of crypto features)

HA (high availability) datacenter and concepts

- 2 independent sites
  - at least 5 km distance (not more than 10 km because of clustering)
- Physical access control
- Power supply
  - dual transformerstation connection
  - Diesel engines
  - Emergency batteries
- Cooling
- Network connectivity
  - At least 2 providers and connections
- Extinguish Fire infrastructure
- Water
  - Detection and prevention of water intrusion

HA (high availability) datacenter and concepts (contd)

- each site represents a production line, ready to bear complete load
  - Network-connection
  - Web-server
  - App-server
  - DB-server
  - Storage
  - HSM
  - App-FW
- active-active configuration
- Web- and App-servers are stateless
- DB is clustered, state is held in DB (Oracle RAC)
- An alternative would be to run the DB active-passive and switch on demand or accident

Stages and staging

- Developer stage (workstation)
- Development and integration stage (centralised build starts here)
- Test stages
  - System Testing (~ 10-15 instances)
  - Performance Testing
- Production stages
  - ISV test reference system
  - Production

- PRESS (Production ReadinESS)
  - Verification that the system can be operated and monitored
    - performance and thruput, tracing, logging
    - failover and recovery

Network, network services, monitoring and SLA monitoring

- GIN = on MPLS level seperated private network, seperated from Internet
  - Guaranteed thruput, next business day service
  - Accepts only GINAs (MAC-address, certificate)
- NTP, DNS, routing
- Firewalls, IDS, IPS
- Loadbalancer (content switch)
- Application firewall (XML-firewall) – IBM Datapower
- Special check services implemented in e-card central system
  - for content switch to verify availability of services per production lines
- Every component and service is monitored
- Consolidated view of availability thru Nagios
  - Service views are neccessary (combination of components)
- Every transaction reports responsetimes (with interim times measured)

Callcenter, Operating & Ticketing

- Callcenter (1st level support)
  - for insured persons
  - for health providers
  - Detailled questionnaires (covers 80-90 % of calls)
- Operating (2nd level support)
  - Resolves the rest of problems or transfers to development, providers or ISVs helpdesk
- Providers (3rd level support)
  - Provider technician resolves issues central or at health providers site
- Development (3rd level support)
  - Resolves and/or finds workaround
- Interconnected thru Ticket systems
  - Each level and unit has it's own ticket system (different requirements)

16

Support of ISVs

- ~ 85 % of HP use specialised software (others use e-card Web-GUI)
- ~ 70 ISVs : ~ 11.000 HP
  - Physicians, Pharmacies, Hospitals, others (medical stores, patient care)
- heterogeneous in skills and technology
- ISVs have to adopt new or changed interfaces at least once a year and deliver it to their customers

- Regular ISV workshops and information to ISVs
- Email and phone support
- 6 weeks before production date we deliver WSDL files, Java-Doc and a reference client implementation

SW Distribution

- 2 Releases per Year
- all interfaces are at least 1 version backward compatible
- No need (because impractible) for a bigbang scenario
- Central server systems are updated with defined downtime
  - Currently not possible to update with zero-downtime (DB !!)
- peripheral: ~ 10,500 GINAs and ~ 15,000 LAN-CCRs

- Currently the first Saturday in May and November => Server deployment
- The following Tuesday to Wednesday night update of 300 selected HPs (guinea pigs)
- A week after (if no problems detected): rollout to ROW

SW Distribution (contd)

- Linux standards for SW distribution not sufficient
  - Need to determine distribution groups
  - Need to define distribution windows (not all of a group should start at the same time to prevent network overload)
- Client administration
  - Group GINAs (by service-type, by location, by distribution time slot)
  - Define distribution order
- SVC monitors state of every GINA during SW distribution
  - Distribution order accepted
  - Linux Download started/finished
  - Linux update started/finished
  - Application download started/finished
 - Ready (or not) !

SW Distribution (contd)

- If someting goes totally wrong ? => Rescue System in place

- GINAs not responding or not fully functional can be rescued
  - Remote (when reachable)
  - Local (Rescue button)
  - Self (when not booting within defined time)

- Worst case
  - Provider technician must visit health providers site

- What, if 10,500 devices are bricks ?

HW-Infrastructure on health providers site (GINA, LAN-CCR, Router)

- GINA
  - Security capsule (crypto, card access, firewall, application firewall, first line of defense)
  - Offline consultation
  - Standalone usage (just a keyboard and a monitor needed)
  - Local application services (end-to-end encryption, local param checks => network roundtrips)

- LAN-CCR
  - Network attached
  - Zero footprint on health providers infrastructure (no drivers needed)
  - multi-user, multi-host
  - Robust, one-hand operation

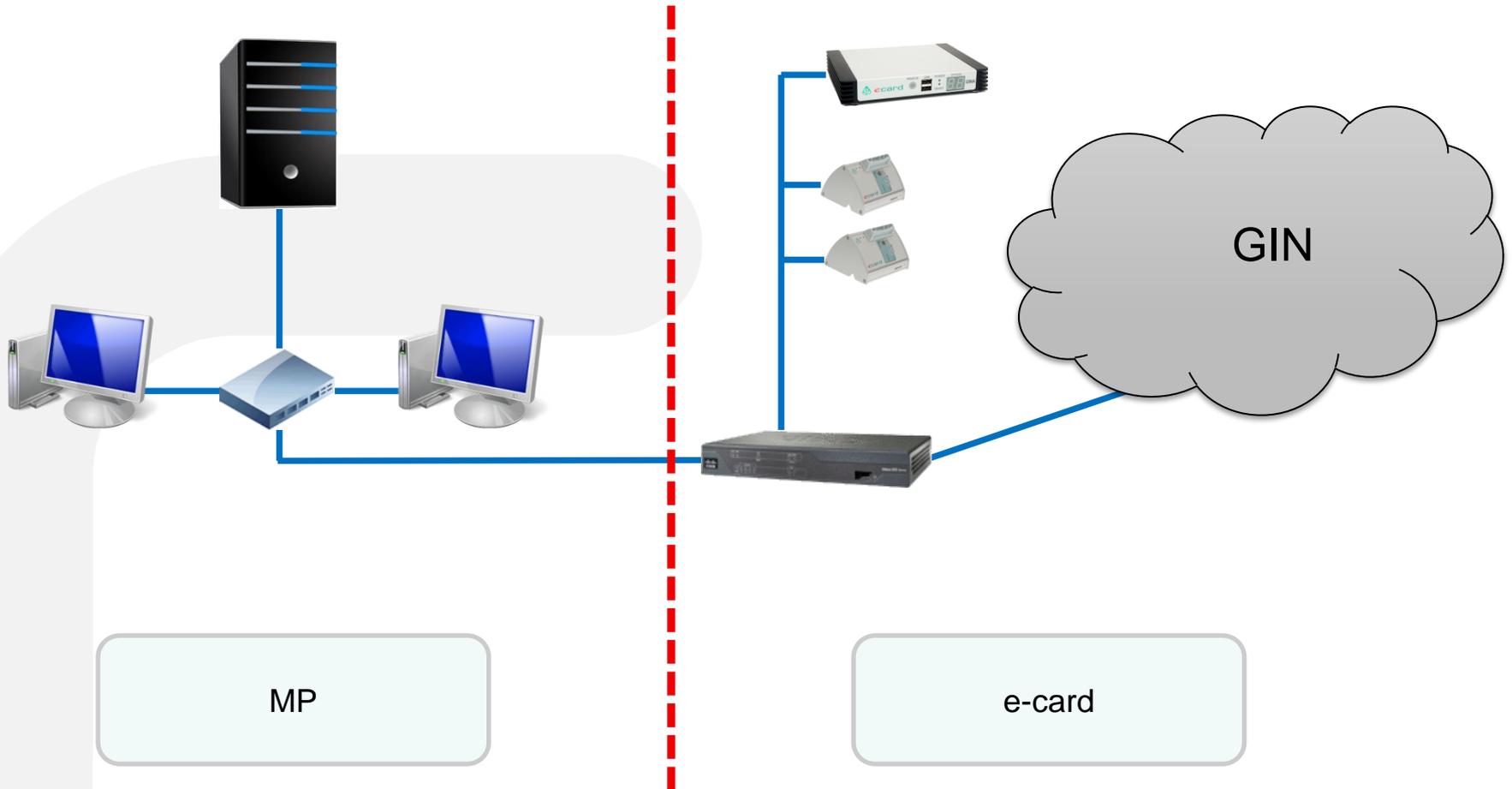# GINA (2nd generation)
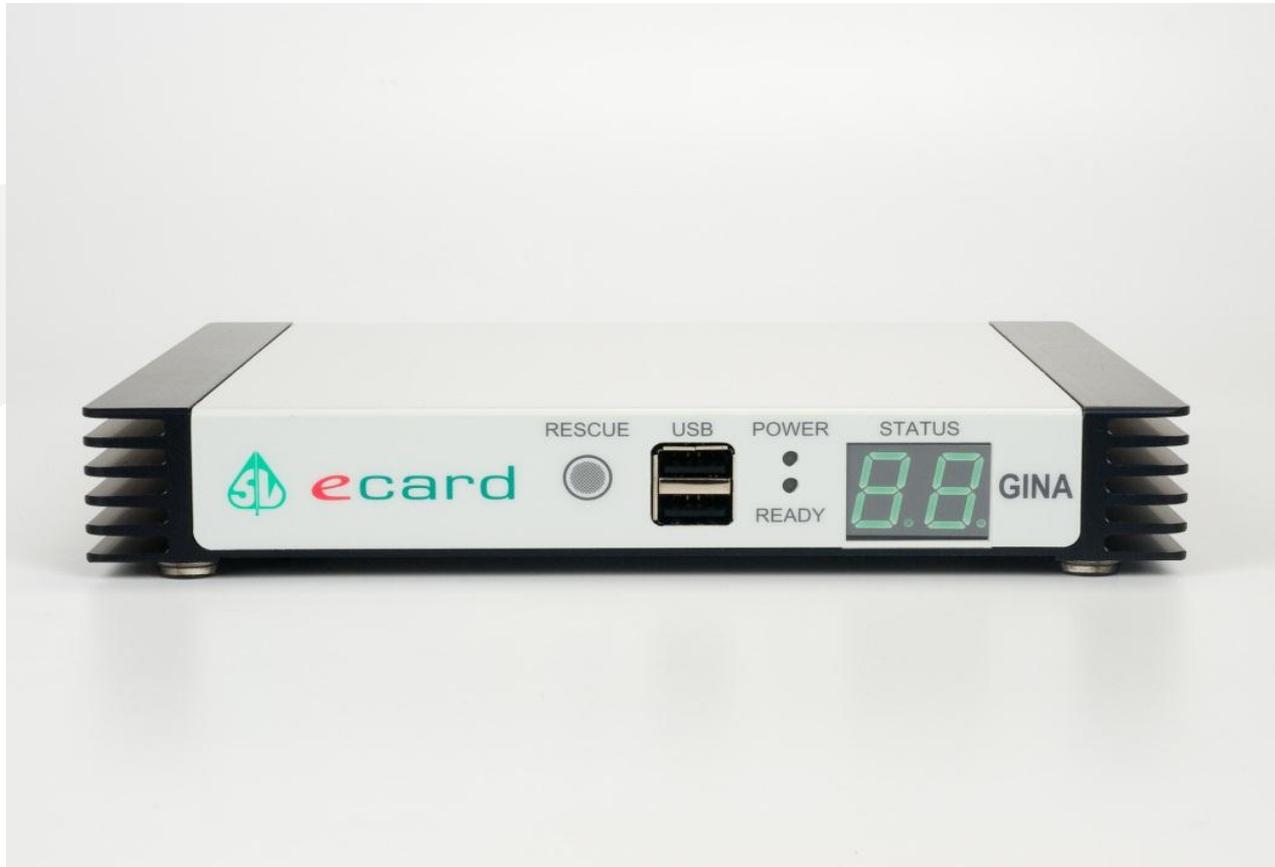
LAN-CCR

HW-Infrastructure on health providers site (GINA, LAN-CCR, Router) (contd)

- Router
  - 2 independent lines
    - GIN => e-card services (ELGA ?)
    - Value added services
      - Secure(d) internet service (AV-Services, content filter, port filter)
      - SW-Distribution of ISVs
      - Medical findings transmission (HP to HP)
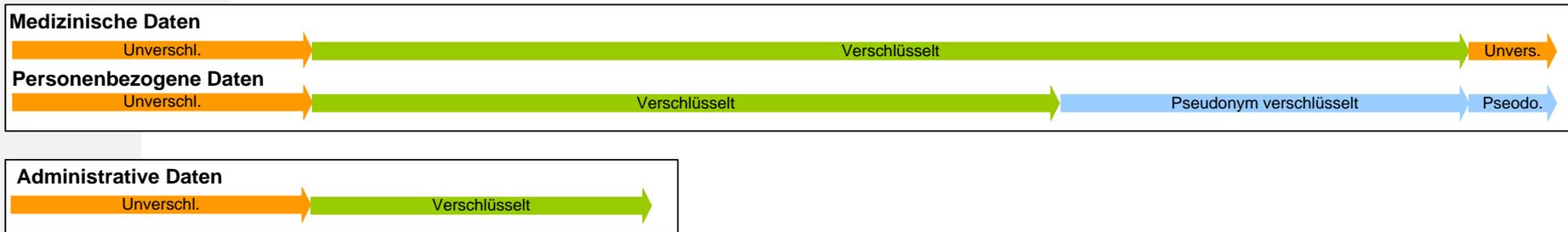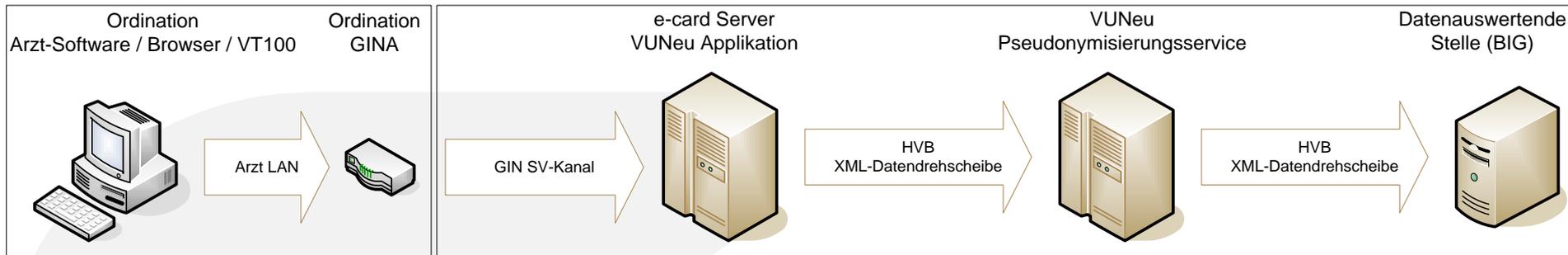   - Health provider's waiting room TV

HW-Infrastructure on health providers site (GINA, LAN-CCR, Router) (contd)

- Mangement of peripheral hardware availablilty
  - SVC tracks availability and error rates of devices
    - Change rates of GINAs and LAN-CCR
    - Watch the „bathtub curve"
  - SVC negotiates provider contracts with HVB
  - every 4-5 years hardware design has to be renewed
    - Minor changes happen earlier
  - Controls major hardware change projects
    - Since Q2 2011: GINA1g => GINA2g (- Q1 2013)
    - currently designing LAN-CCR2g

Responsibilities at MP's premise

GIN

MP

e-card

Pseudonymisation

Ordination Arzt-Software / Browser / VT100	Ordination GINA	e-card Server VUNeu Applikation	VUNeu Pseudonymisierungsservice	Datenauswertende Stelle (BIG)

Medizinische Daten
Unverschl. → Verschlüsselt → Unvers.

Personenbezogene Daten
Unverschl. → Verschlüsselt → Pseudonym verschlüsselt → Pseodo.

Administrative Daten
Unverschl. → Verschlüsselt

- Medical data and meta data separated and separatly encrypted

27

Security Token Service

- e-card system is (and will be in ELGA) a trusted identity and „contact" provider
- SAML based STS tickets for
  - Identifying a MP
  - Asserting a MP patient contact
- Today used for Web-Portals of some hospitals
- When a doctor wants to authenticate himself, he requests a ticket from the e-card system => hands over STS ticket to Service (ELGA), which then decides, whether and what rights the doctor has
- When he wants to access patient's data, requests a ticket from the e-card system to proof the contact (e.g. consultation) => hands over STS ticket of Service (ELGA), which tehn decides on policiy and consent of the patient, what documents the doctor will get to know

What's next ?

- Currently waiting for ELGA (Austrian nationwide EHR project)
  When ELGA law passes parliament
  – eMedication application of ELGA

- Long list of social security processes waiting to be changed from paper based to electronic processing
  – further electronic approval services (other than medication) - EBS
  – ePrescription - eRezept
  – electronic assignment of patients to other MPs - UZE

Q&A

Rainer Schügerl

SVC

Head of Development, CSO

rainer.schuegerl@svc.co.at