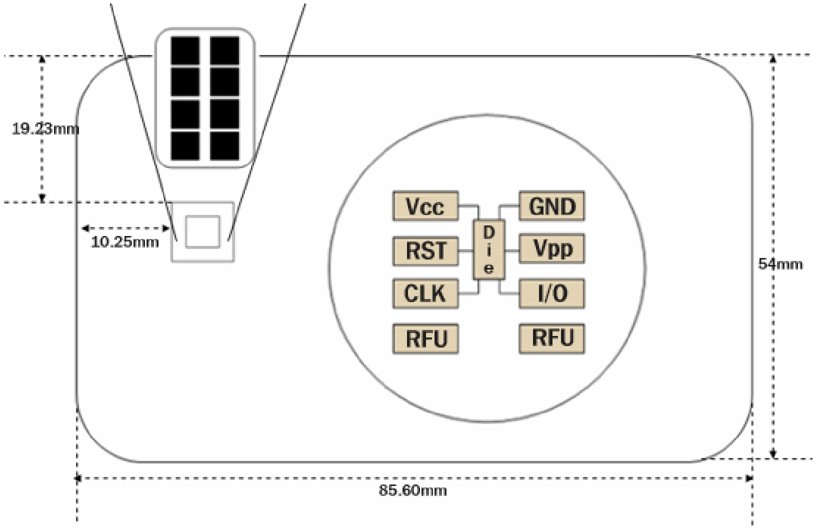
Smart Cards – Technology and Application

Silvio Svečnjak <silvio.svecnjak@fer.hr>

Contents

1. Technology Overview
2. Applications
3. Implementation - Local
4. Implementation - System
5. Conclusion

Technology Overview



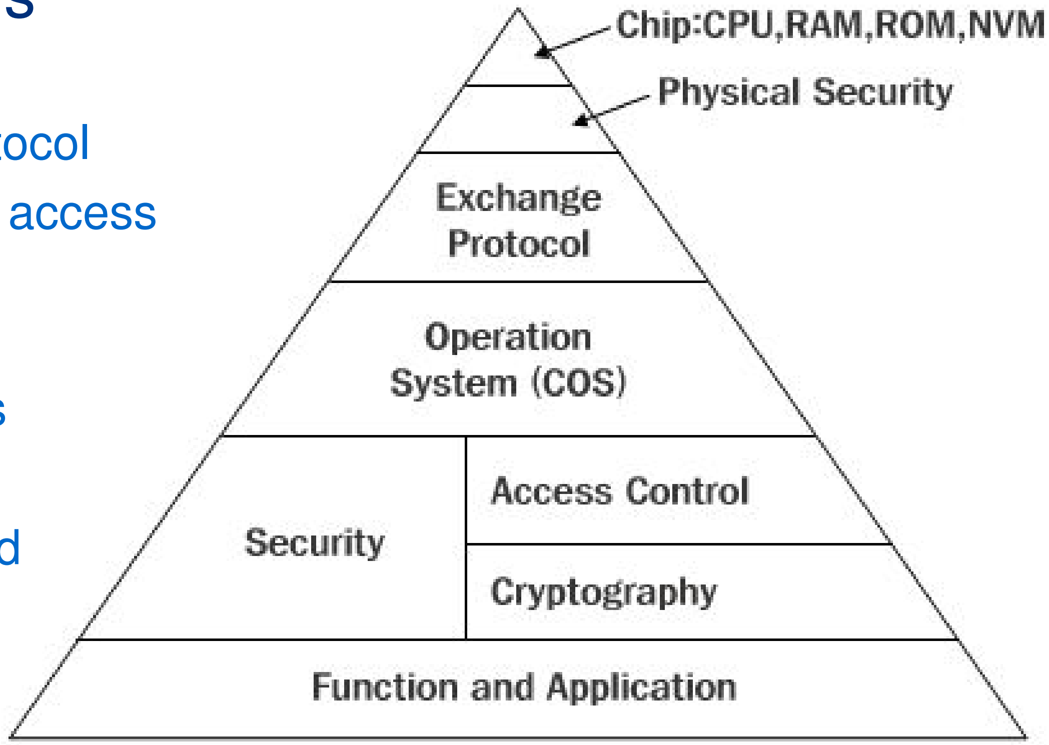
Basics

- Standards ISO 7810, 7816/1 i 7816/2 7816/3
- Microprocessor + I/O controller + memory - ROM, RAM, NVM
- Serial communication – T=0, T=1 protocols (ISO 7816/3)
- Types – contact, contact-less – hybrid or dual interface
- Built in OS – MULTOS, JAVA, proprietary
- Durability

Technology Overview

Security mechanisms

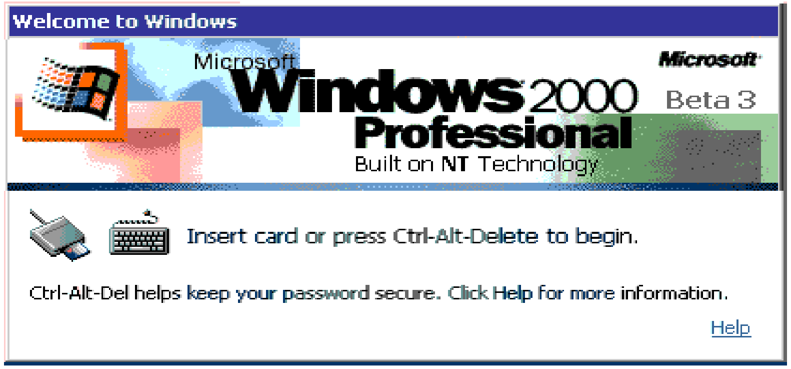
- Self containment
- Communication protocol
- OS security – folder access restriction
- PIN protection
- Encryption protocols
- Application security
- 2 side terminal - card authentication



Applications

- Authorisation
  - Entrance authorisation
  - ID cards
- Authentication
  - Storing password(s) for system log on
- Accounting
  - Bank cards, credit cards
  - Shop loyalty cards
  - E-wallet card
- Encryption
  - Storage of secret key(s)
  - Digital signature for documents

Implementation - Local



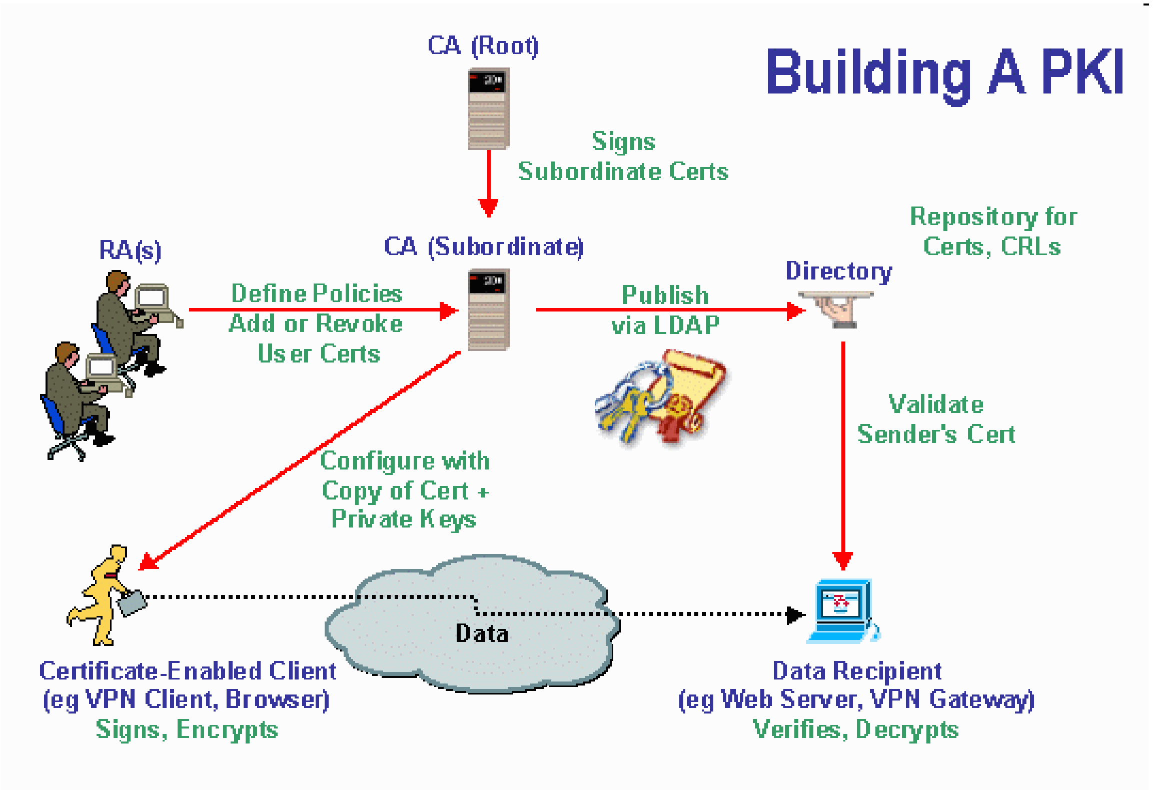
Insert card or press Ctrl-Alt-Delete to begin.

Ctrl-Alt-Del helps keep your password secure. Click Help for more information.

Authentication

- Where?
  - Security sensitive environment
- Why?
  - passwords written on post-it, or made simple so they can be remembered
  - saves maintenance time (password issues)
  - 2 way protection – possession of a card + PIN
- 2 modes – password(s) / PKI + certificate
- Infrastructure: multiple PC card readers, card reader driver software, administrating software

Implementation - Local



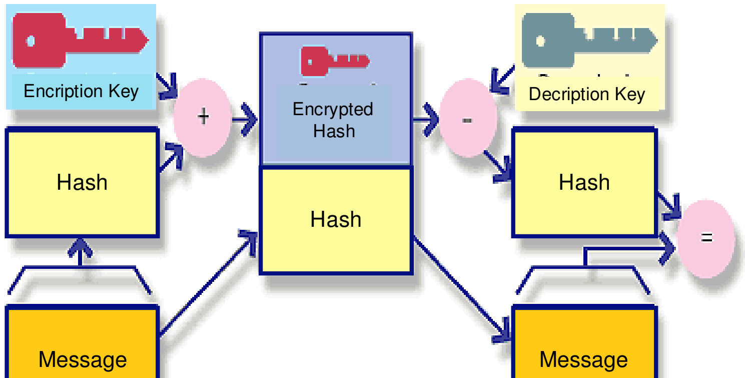
Encryption

- PKI – public key infrastructure
- Digital certificate available
- Private key – stored on a smart card

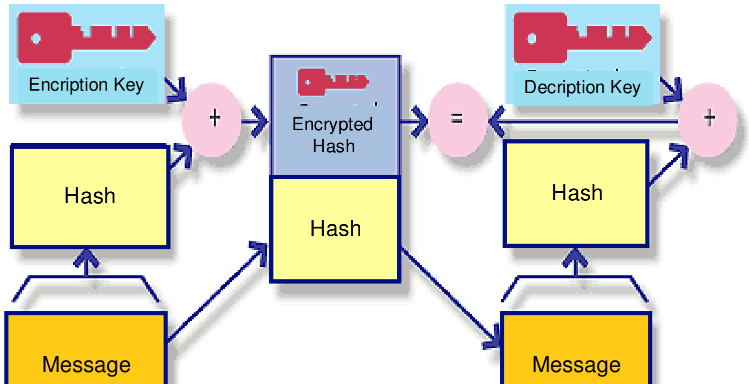
Implementation - Local

Digital signature

- Lawfully accepted way to sign electronic documents
- Provides:
  - Signer authentication
  - Document authentication



Digital Signature - PKI

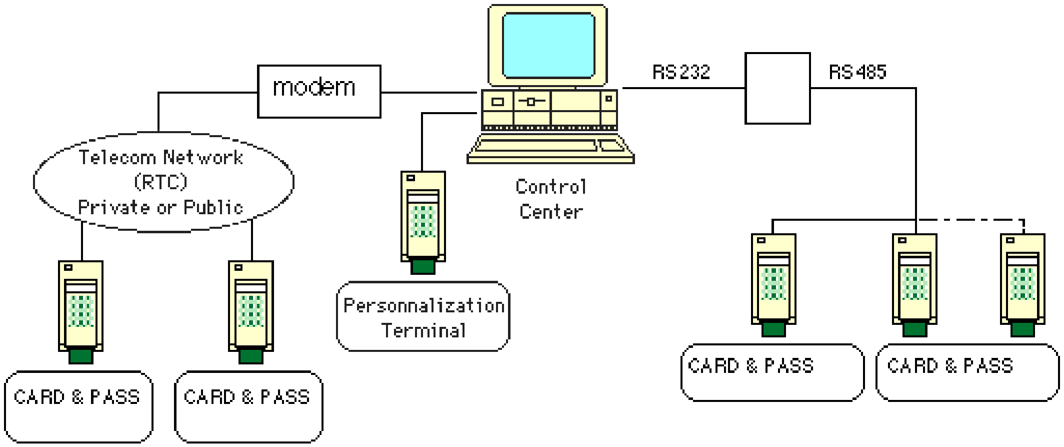


Digital Signature – shared private keys

Implementation - System

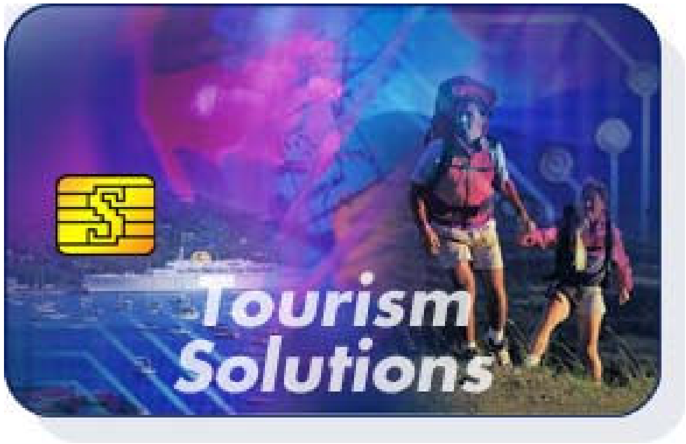
- **Entrance authorisation**
  - Where?
    - medium and large companies
    - parking areas
  - Why?
    - Entrance/exit time control
    - Attendance control
    - Implementation of complex access restriction policies
    - Simple use, faster than key(s)
    - 1 card can replace several keys
    - Card costs less than secure key

Implementation - System



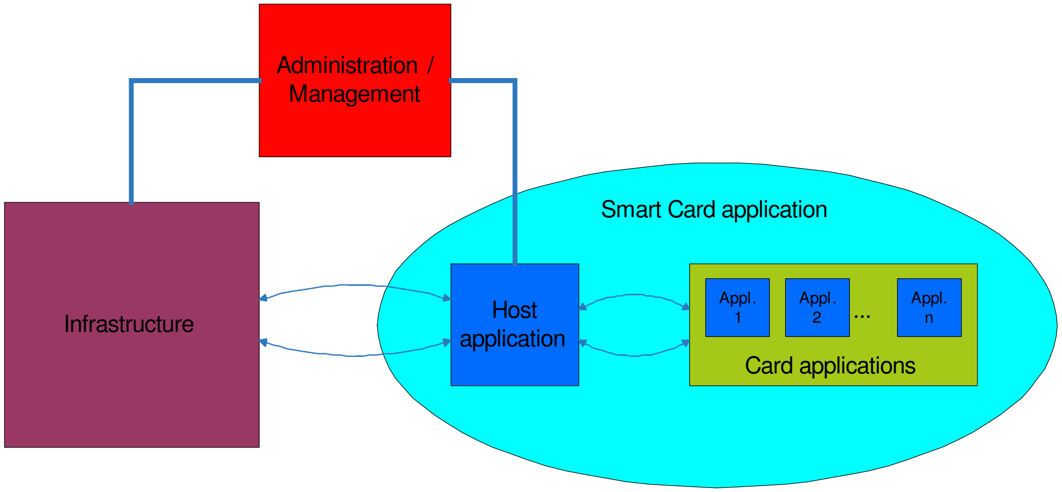
- **Entrance authorisation**
  - Infrastructure – multiple card readers, interconnection network, server + database, control/management software, electronic locks/doors
  - Issues
    - network infrastructure expensive
    - control/management software – expensive if customisation is required

Implementation - System



- **Tourist Resort Card**
  - Where?
    - Any closed resort, swimming pool, camp, etc.
  - Why?
    - User convenience, better quality of service
    - All inclusive card - entrance authorisation, e-wallet, loyalty
    - No need for cash, credit cards, keys - increased security for guests
  - Multiple independent applications on 1 card
  - 1 integrated host application
  - “Of the shelf” solution doesn’t exist

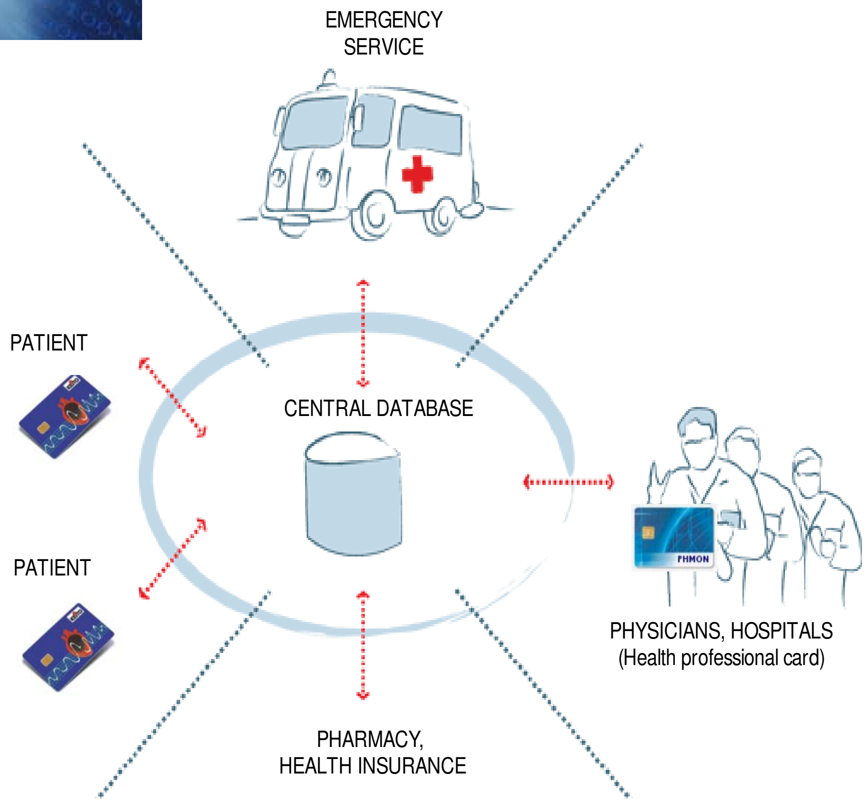
Implementation - System



Tourist Resort Card

- Implementation
  - Network infrastructure – LAN, WLAN, GPRS
  - Terminals – POS terminals, contact-less, user kiosks
  - Central storage/application server + database,
  - System administration/management software
  - User software – reception desk, user kiosks
  - User training

Implementation - System

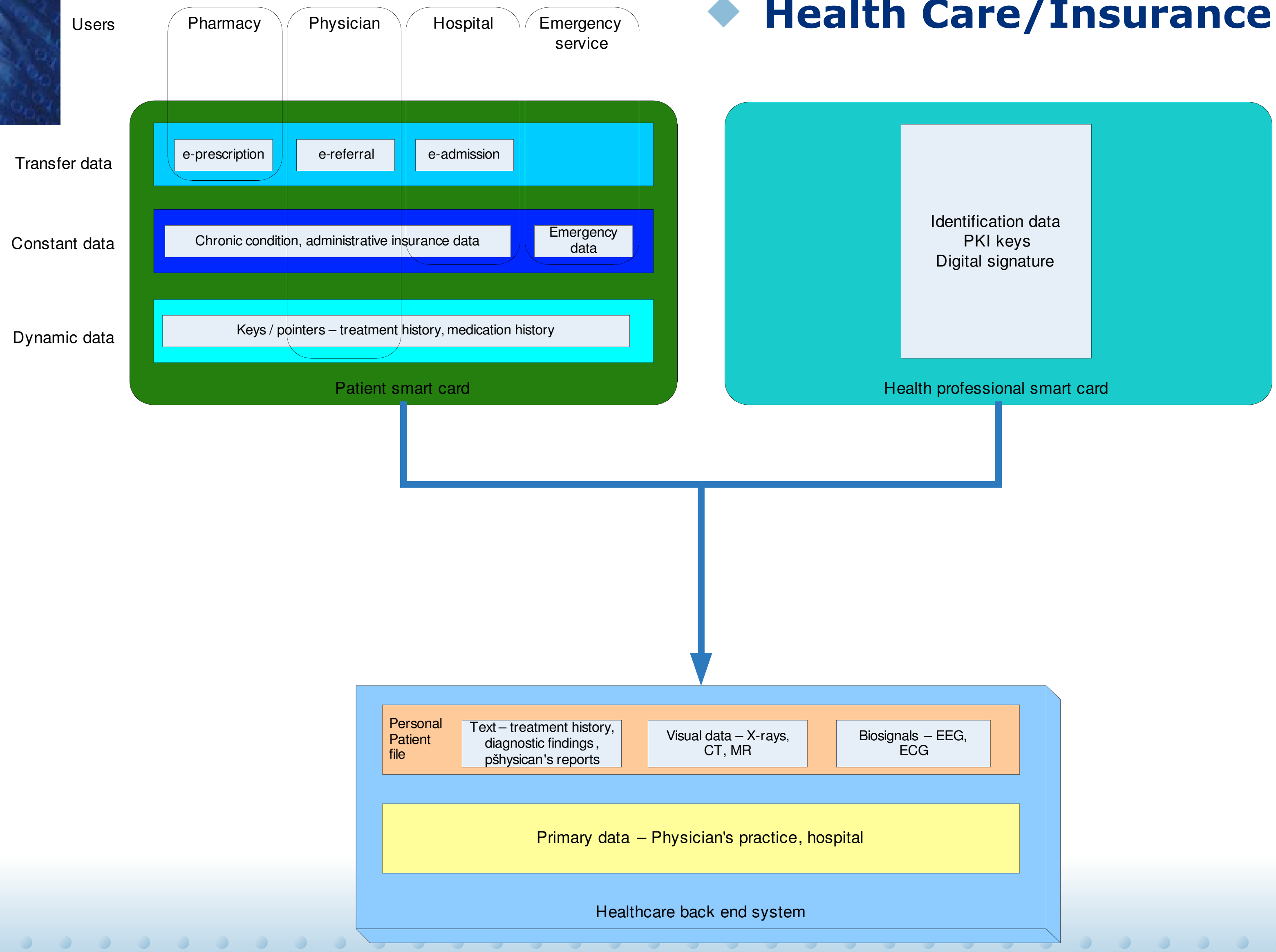


Health Care/Insurance System

- Where?
  - Large national health insurance systems
- Why?
  - Better control for fraud
  - More efficient payment/reimbursement
  - Confidentiality of health data
  - Saving on issuing new cards – data updateable
- 2 major approaches:
  - Smart card used for health insurance purposes only
  - Smart card used for:
    - Storing health insurance data/status
    - Storing medical data
    - Health information system access

Implementation - System

Health Care/Insurance System



Users

Pharmacy

Physician

Hospital

Emergency service

Transfer data

e-prescription

e-referral

e-admission

Constant data

Chronic condition, administrative insurance data

Emergency data

Dynamic data

Keys / pointers – treatment history, medication history

Patient smart card

Identification data
PKI keys
Digital signature

Health professional smart card

Personal Patient file

Text – treatment history, diagnostic findings, pšhysican's reports

Visual data – X-rays, CT, MR

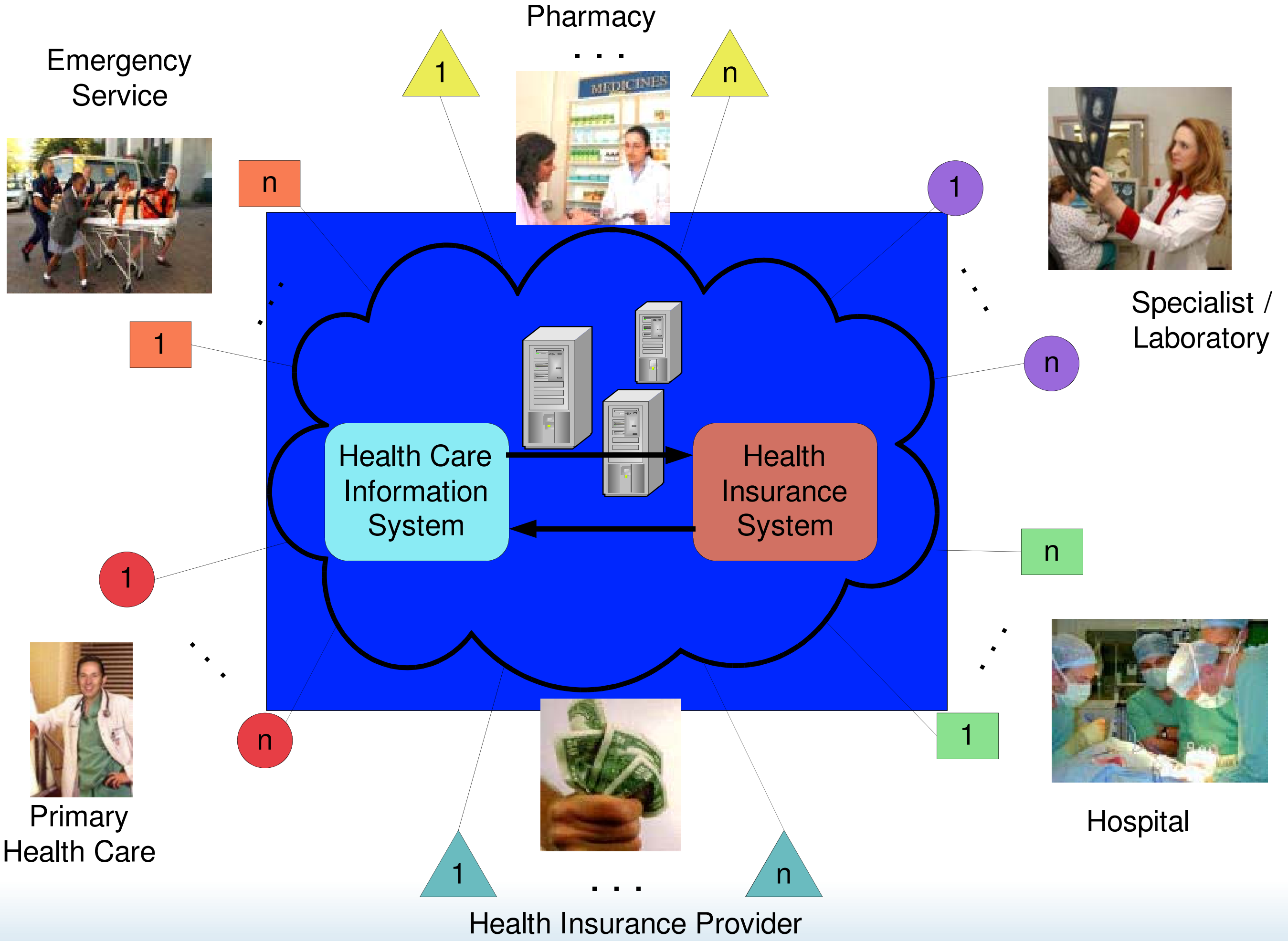
Biosignals – EEG, ECG

Primary data – Physician's practice, hospital

Healthcare back end system

Implementation - System

Health Care/Insurance System



Conclusion

- **Smart cards have actually become "smart" – OS + multiple applications**
  - Versatile
  - Secure
  - Convenient
  - Cheap
- **Technology still evolving**
  - Card production still expensive
  - Only a few major vendors
  - Card – reader incompatibilities common
  - Smart card – PC framework not completely standardised
  - Card application development limited by lack of standards
- **Smart card systems – expensive**
  - Existing solutions often not flexible enough – customisation expensive
  - Only large customisation projects economically justified due to vendor incompatibilities
  - Infrastructure costs often overlooked