



eHealth Foundation Bulgaria

NATIONAL CONFERENCE

Enforcing of Standards in the eHealth Area.
Integration of Information Systems,
Interoperability and Protection of Personal Data.

**“Basic Functions of an Electronic Health Card
from a Conceptual Point of View
and Implementation / Infrastructure Alternatives”**



Reinhold A. Mainz, Independent ICT / eHealth Consultant, Germany

Short Term Expert (Adviser)

*EU funded Twinning Project Bulgaria – Germany “Free Movement of Workers”:
Electronic European Health (Insurance) Card*

Basic Functions of an Electronic Health Card from a Conceptual Point of View

- Description of a SmartCard for eHealth applications
- Analysis
- Conclusions
- Remarks
- One last but important question
- Recommendation

Description of a Smart Card for eHealth Applications (1)

- Computer
- Processor with **secure operating system**
(runs special software / firmware)
 - Resources manager
 - Remote access, authentication procedures
 - User access
 - eService access

Description of a Smart Card for eHealth Applications (2)

- Storage with secure storage concept (restricted access)
 - Device data
 - **Cryptographic keys**, PINs, biometric data
 - Application related software / firmware

Description of a Smart Card for eHealth Applications (3)

- Documents
 - Data to support authentication (**certificates**)
 - Derive rights for access to data, applications, services, infrastructure
 - Identification data
 - **Attributes**

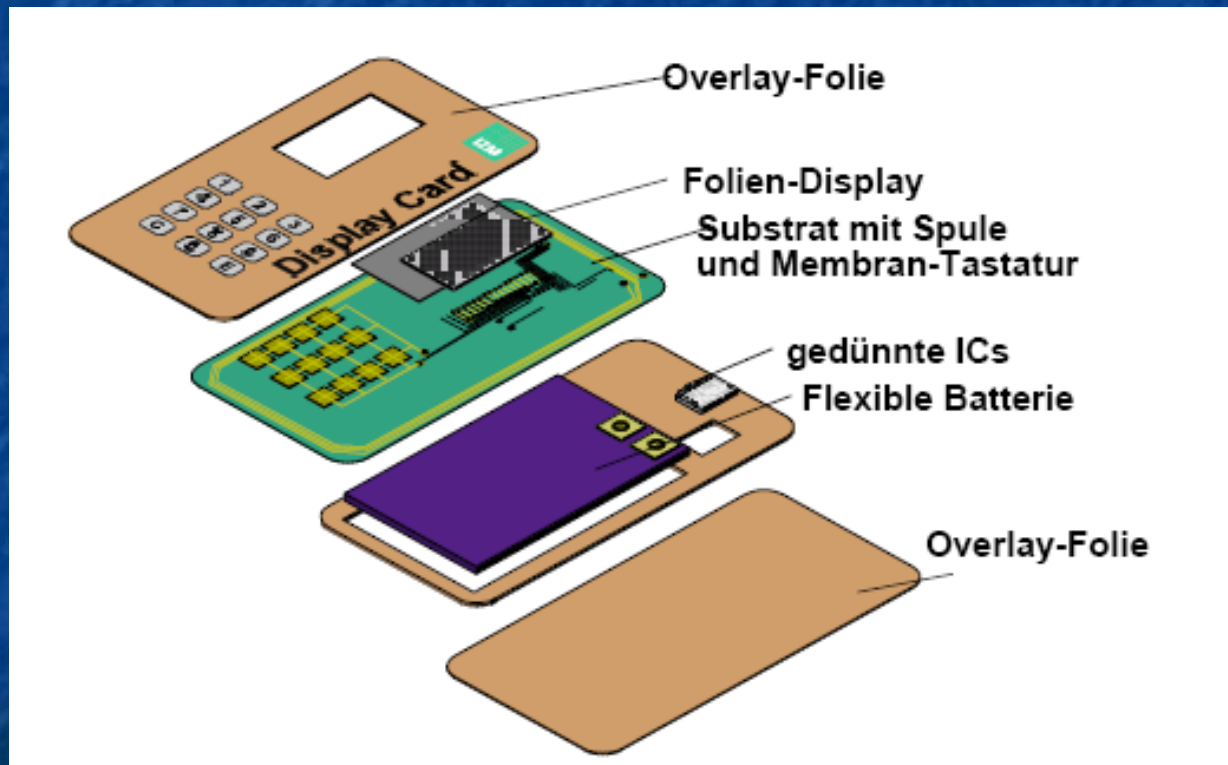
Description of a Smart Card for eHealth Applications (4)

- Application data (static / permanent or temporarily)
 - Administrative
 - like how insured
 - Clinical
 - Health status
 - Emergency data
 - Keys and links to personal electronic health records
 - Documents for transport
 - Prescriptions
 - Test results
 - Discharge letters

Description of a Smart Card for eHealth Applications (5)

- No **human interface** or a **primitive** one
 - Input via card reader
 - Output via card reader
 - Update via card reader
 - Input by pressing a single key (button)
 - Output by a rotating display

SmartCard with button and display



Description of a Smart Card for eHealth applications (6)

Used "Offline" or "Online"

"Offline":

- Data is provided by the SmartCard itself in interaction with local hard-/software that enters commands into the SmartCard and gets results

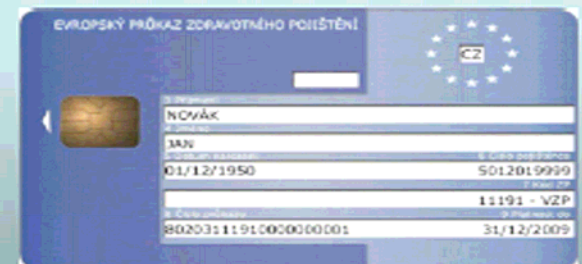
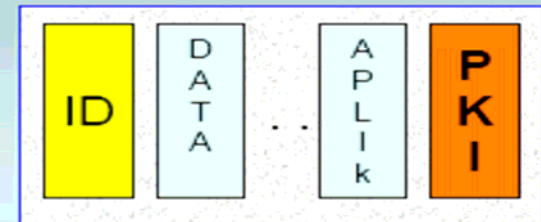
"Online":

- Data is provided by the SmartCard in collaboration with other computers (local or in a network)
 - Most services will be network based, smart cards can store some synchronized data
- **The only data that must be used "Offline" are the private keys of an PKI (Public Key Infrastructure)**

Example of an eHealth SmartCard

Results of Electronic Identifier Analysis

1. EI will have a form of a smart card, and will serve for both visual and electronic identification of the insured.
2. EI will be compatible with the eEHIC concept.
3. EI will bear selected health data of the insured, mainly, however, it will be a key to all information stored outside of the card.
4. EI will also be used in the area of social services.
5. EI can be a host to other suitable applications.



VZP ČR

8

Analysis

- Only application data is domain specific
- Storage place (locality) of application data normally is not relevant
- If application data shall be available "offline" (read from the SmartCard) in principle it can be synchronized at every time with online connection
- Storage of application data on a SmartCard is useful if it is the only foreseen storage place (esp. for some security reasons) or as a precaution for not available networks

Conclusions (1)

- A SmartCard is a (the!) **security tool** for cryptography (authentication, encryption/decryption, Digital Signature) esp. in an PKI environment
 - main function is to **hide private keys** of a key pair (coupled by an secure algorithm) and to **use a private key in a secure environment**
- A SmartCard can run very small algorithms and use data to do it whether stored on the card itself or not
- The user interface (human interface) is primitive and normally needs a local computer with better human interface

Conclusions (2)

- Minimum human interface might be a button / a very small keyboard and a very small display
- A SmartCard is a mobile tool, therefore **a combination with a mobile computer** (PDA, Mobile Phone, ...) **can bring an acceptable human interface** and additional (storage) resources, but raises up the infrastructure price.
- Standards for SmartCards should only be SmartCard depended if really needed (!), all other standards can and should be **general standards** for computer usage, esp. standards for application data communication

Conclusions (3)

- from an eGovernment point of view a citizen's **SmartCard should be application independent**
 - no application data on the card, or
 - application data for different domains
 - From a generic point of view **the citizen itself could / should define which data shall be synchronized** with the SmartCard application storage (possible as long as there is sufficient storage space)

Conclusions (4)

- A SmartCard can be a **digital passport** (to be used as part of an PKI) with data by decision of the citizen
 - **Attributes of the citizen can / should be stored in PKI certificates**
 - there is **no need to store PKI certificates on a SmartCard** itself, certificates are movable documents, secure by digital signature
 - Identifiers for special applications can / should be stored in application depended Attribute Certificates
 - **data protection issues can be solved by using different application oriented identifiers stored in different certificates**
 - Storage of the Public Key by applications could be forbidden, a Public Key can / must be used only by cryptographic algorithm

Conclusions (5)

- The society (state) has to decide or can decide for what reason **one - or more than one - SmartCard** for every citizen shall be issued - and by whom
 - digital passport
 - health insurance card
 - health card
 - electronic European Health (Insurance) Card
 - banking card (s)
 - card to pay for public traffic usage
 - ...

Conclusions (6)

- **Implementation** shall be **SmartCard independent** as wide as possible
 - Infrastructure might differ from domain / organisation / country to ... and can change in the future
 - will there be a SmartCard in the next technology generation?
 - Usage of a generic framework architecture
 - Usage of generic design principles for ICT solutions

Remarks

European wide (global) interoperability needs

■ Standards

- policy agreements (treaties)
- Organizational agreements (contracts)
- Common semantic understanding
- Technical standards
 - meta level
 - application level

■ Common infrastructure (s)

- **policy agreements** (treaties)
- Organizational agreements (contracts)
- Interoperability proofs

Political / Legal

Organisational

Semantic

Technical

Layer Model of ID Management

Political / Legal

Legislation, nomination of responsible authorities, definition of covered entities

Organisational

Registration procedures, verification procedures

Semantic

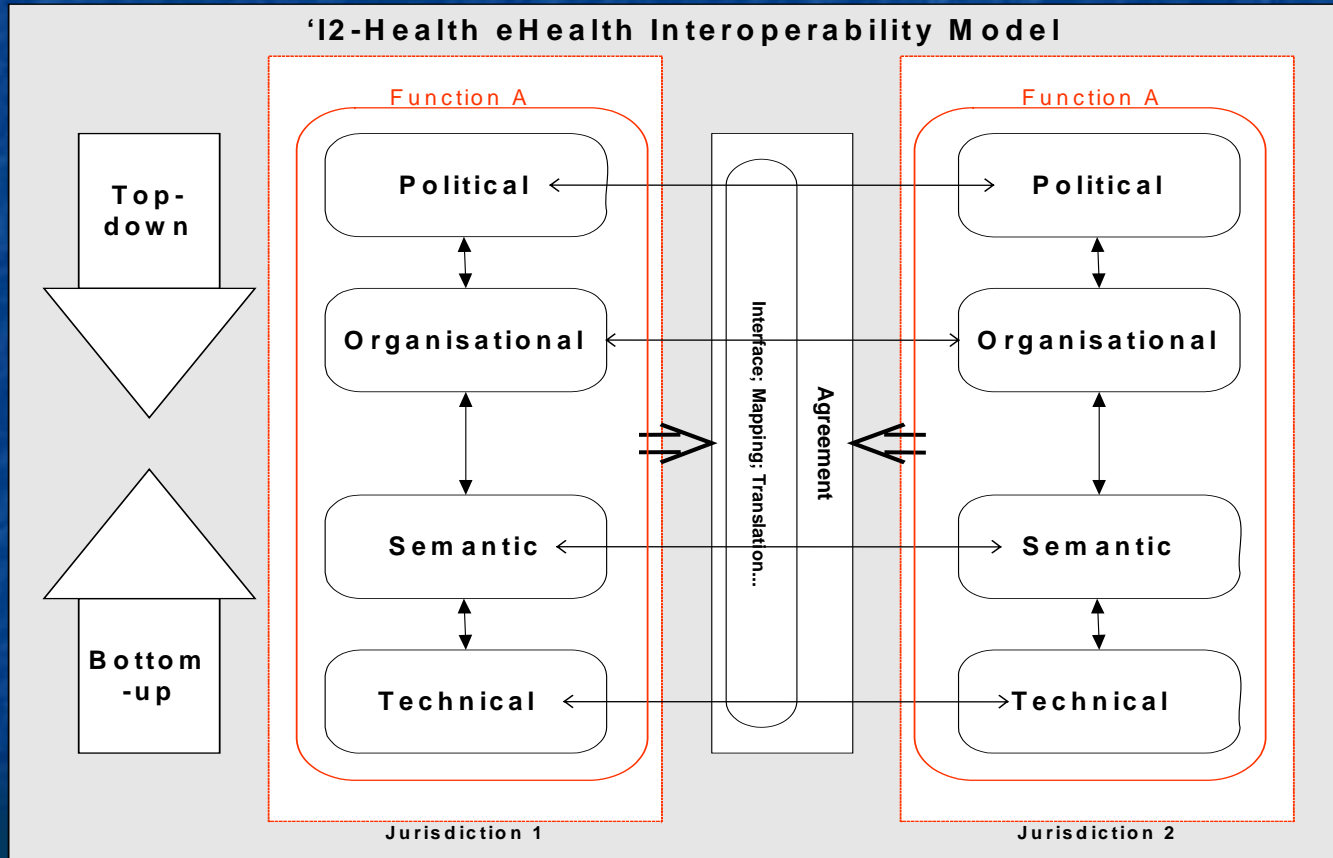
Data models, identifiers, numbering systems

Technical

Certificates, ID-tokens (e.g. cards), directory databases, networking infrastructure

- *What is the legal base for issuing/using the identifier*
- *How is the registering process organised?*
- *Which identifier is to be used?*
- *On which support is the identifier available?*

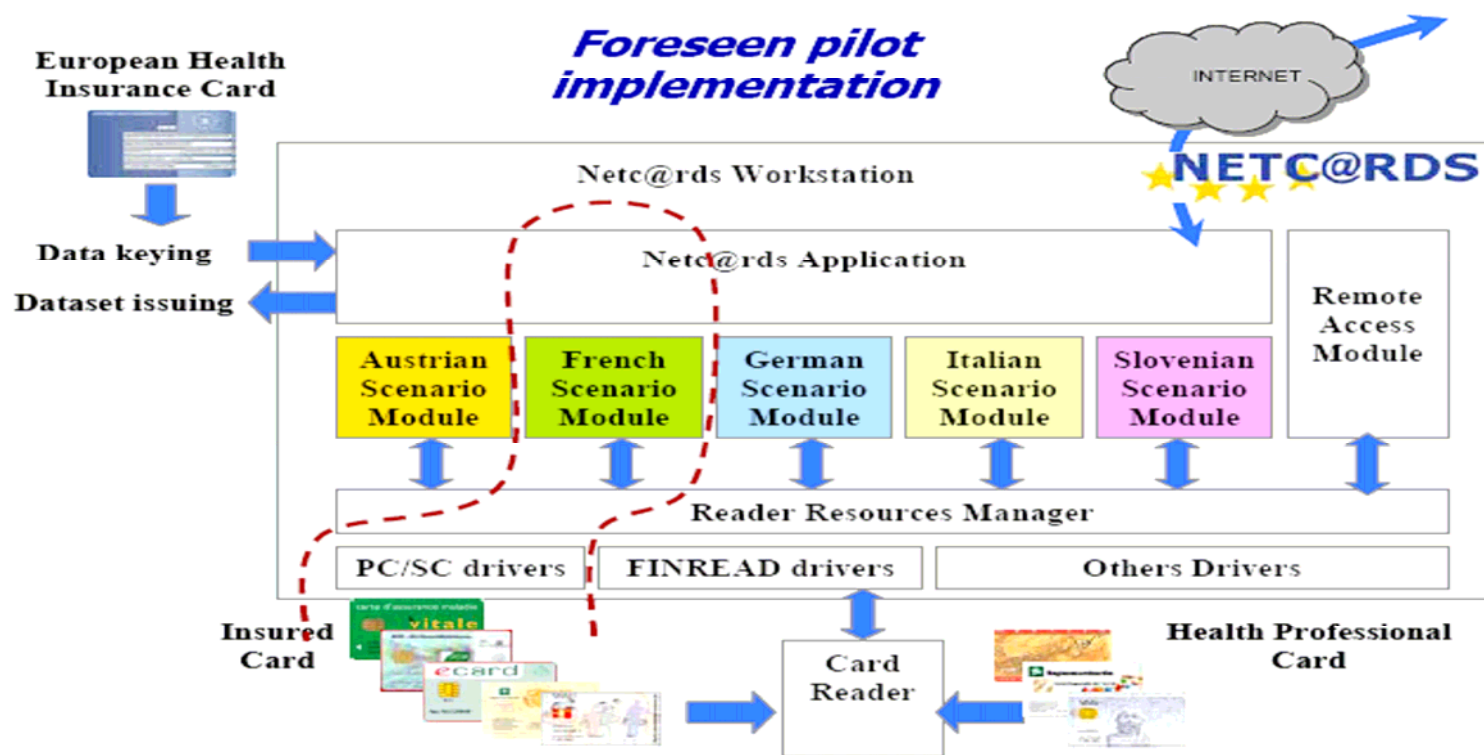
Interoperability Model



I2Health

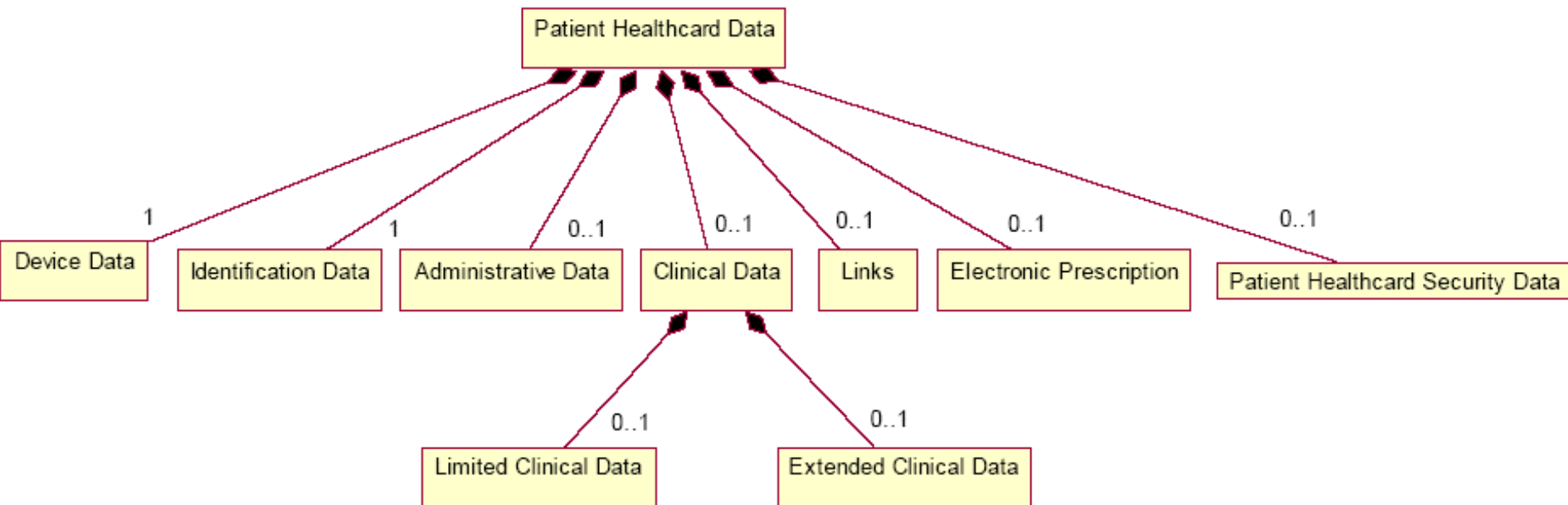
Interoperability with different national SmartCard solutions

Card/reader interoperability ...



International health card standard (norm)

ISO 21549



Interoperability with different national access rights / mechanism

Cross-border access to personal data

- ▶ Security measures aiming at restricting access to some data to only authorised persons may be
 - A PIN code under the sole control of the cardholder
 - The mutual recognition of the patient and health professional cards
 - A strong authentication (PKI-based) mechanism
- ▶ The interoperability problem
 - Some data may be of restricted access in some MS while of open access in others
 - Access restrictions may be subject to different level of security
 - Interoperability agreements are necessary for managing security gaps
- ▶ Technical interoperability for
 - Strong authentication is in progress

Marc Lange, EHTEL

One last but important question

- Do and can we in the European Union accept different solutions for eHealth infrastructures from different Member States, like
 - Health Card
 - Health Insurance Card
 - Digital passport
 - Authentication with a portal solution
 - mobile computers
 - ...



Use collaboration in Europe on all levels

- Know how transfer
- Avoiding mistakes on the design and architectural level
- Common understanding
- Interoperability
 - Organisational procedures
 - Infrastructure
 - Applications
- Perhaps funded by a EU programme

Recommendation

Use collaboration in Europe on all levels

- Know how transfer
- Avoiding mistakes on the design and architectural level
- Common understanding
- Interoperability
 - Organisational procedures
 - Infrastructure
 - Applications
- Perhaps funded by some EU programme

Questions?

I ■
C ■
T ■
E ■
H ■
E ■
A ■
L ■
T ■
H ■

Dipl.-Inform. Reinhold A. Mainz
BERATER (CONSULTANT)



UNTERM BEGGENBEIL 18
58802 BALVE
DEUTSCHLAND (GERMANY)

TELEFON + 49 2375 939 973
TELEFAX + 49 2375 939 974
MOBIL + 49 175 2 239 110

E-MAIL REINHOLD.A.MAINZ@GOOGLEMAIL.COM

