



BIS | Department for
Business Innovation & Skills

ISG
Royal Holloway
University of
London

Security measures, benefits and challenges of the Finnish EHR and National Health Information Infrastructure

- a road-map from principles to trusted EHR sharing

IT security for e-health workshop

Friday 4th September 2009, Royal Holloway, University
of London, UK

Pekka Ruotsalainen
Research professor (THL)
Adjunct professor (Univ. of Tampere)

Themes discussed

1. Facts about the Finnish health care
2. The Finnish eHealth strategy
3. Security concepts, principles and legislation for eHealth
4. The Finnish EHR-model and its security features
5. The roadmap to trusted national use of the EHRs in Finland
6. Security architecture, functions and services of the Finnish NHII
7. Challenges and remaining problems

Finnish Health Care in Brief

- 5.3 million inhabitants
- Municipal responsibility to organise services (370 municipalities)
- Highly **distributed** service system
- Mixture of **public and private** services
 - Private sector covers 25-30 % of GP and specialist visits
 - Private Pharmacy system
 - Private occupational care system
 - Public secondary (hospital) care
 - 200 public primary care stations (50% have also bed units)
 - 20 Secondary care hospital districts
- 17.000 medical doctors (6000 working full time in private sector)



The Finnish eHealth strategy

THE FINNISH STRATEGY FOR eHEALTH

- a 12 year journey

First strategy published 1996. Main targets:

- From institutional care to citizen centric continuum of care model
- Digitalization of all health records
- Regional healthcare information systems (RHIS), which support cross organisational seamless service chains
- Cross organisational EHR sharing
- High level of security and privacy

The Finnish Journey to national eHealth services...

- 1999-2003 5 regional EHR-systems was implemented.
- 2004-2006 An updated national eHealth architecture.
New eHealth legislation, and the selection of national standards.
- 2007-2013 The implementation of National architecture..
First steps to semantic interoperability.
The eHealth 2010 road-map (for EU).
- 2013- Target: NHII fully functional (e.g. EHR sharing and ePrescribing)
Selected national eHealth services for citizens

Main eHealth targets

- Better availability and quality of care by using 100% digitalized EHRs and the NHII
- Wider secondary use of information for purposes based on the public interest (e.g. identification people under risk)
- Cost reduction
- Support for cross-organizational continuum of care services
- Availability of EHRs 24h/7d anywhere
- Trusted use and sharing of EHRs
- E-services supporting self care and personal wellness management
- Citizen access to his/her own EHRs via the Internet and mobile networks
- Open platform for value added eHealth applications

Security concepts, principles and legislation for eHealth

Framework for trusted IT-systems in health



Security and privacy principles for eHealth

Any use of the EHR should be ethical and fulfil regulatory requirements

1. General principles

- The *information privacy* principle means that individuals and patients can determine themselves, when, who, how and to what extent information about them is communicated to others excluding situations where there a specific legislation allows the use of the EHR.
- Security including confidentiality, integrity, availability, accountability of information. Also non-repudiation of communication and event should be proven

2. Main health care specific concepts and principles:

- (patient-doctor) Relationship is needed for any access to the EHR or there must be a specific legislation enabling the access,
- Patients can use consent and/or opt-out to restrict the use of his/her EHR within limits of national legislation,
- A legitimate purpose is needed for any access otherwise there should be a specific legislation enabling the access and use of the EHR,
- The health professional can override consent, opt-out and purpose rules in specific situations (e.g. to save patient's life),
- Only persons participating in the care of treatment have permission to access the content of the EHR,
- Patients have rights typically defined by national legislation (e.g. the Act on Patients Rights). Typical rights are: right to access own EHRs, be informed and use consent/opt-out,
- Health professionals have responsibilities as: enter relevant information to EHRs (responsibilities are defined at the level of a degree),
- The service provider organisation has responsibilities (e.g. maintain and archive EHRs).

Main security and privacy risks created by the NHII

- Integrity of the EHR is not proven during communication and preservation,
- The content of the EHR is made available or disclosed to unauthorised individuals or computer processes,
- Non-repudiation of communication (e.g. data origin is not proofed, there is a false sender or receiver and false data content)
- Non-repudiation of events
- Expanded secondary use of EHRs for other than medical purposes
- The use of EHRs without patient- doctor relationship
- Poorly defined roles and access control rules

Principles guiding the use and access of EHRs in Finland

- The service provider organisation (the GP, health station, health care centre, hospital or hospital region) has the responsibility to manage and archive EHRs in trusted way.
- Consent is not need for the access to EHRs inside the service provider organisation in the case the person have the status of patient.
- Any data disclose between service provider organisations require patient's consent - or there should be a legislation enabling the data disclose.
- The service provider organisation has right to define which persons are participating the care process and having access to patient's EHR.
- The responsible physician have by specific medical reasons right to hide selected parts of the EHR from the patient.

Citizen or patient have the following rights:

To be informed:

- To know how the NHII manages his/her records

To control the access and disclose of his/her EHR:

- Limit the access and disclose using consent and opt-out
- Change any time consent and opt-out decisions/rules
- Define if paper prescriptions should be used

To check audit-trails:

- To know in the case of any EHR disclose, who, when for what purpose and to whom his/her EHR has been disclosed

Present regulatory framework for security and privacy protection (an eHealth view)

EU-level regulation:

- EU data protection directive
- EU e-signature directive

Generic national legislation: Constitution of Finland

- Data protecting in electronic communication)
- Act on Archiving
- Act on personal data protecting
- Criminal law
- Act on services in the information society
- Act on electronic communication on the duty
- e-signature act

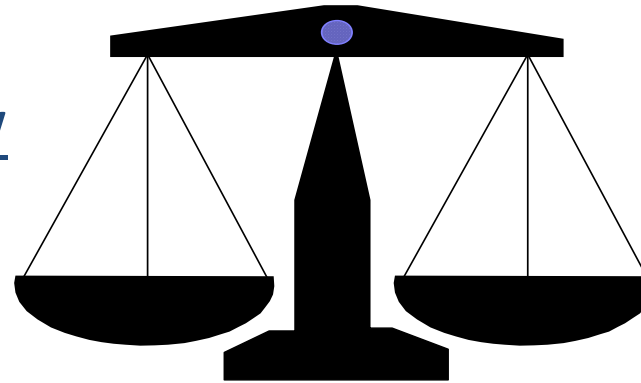
Healthcare specific laws and decrees

- The act on patient's rights
- Decree on the information entered to the patient record
- Act on the management and use of electronic patient information
- Act on e-prescribing

The Act on the Management and Use of Electronic Health and Social Welfare Information defines a new balance between privacy and availability

Health Professional's view

- EHR browsing
 - Access permissions
-
- Demand of the relationship
 - Legitimate purpose
 - Access rights are restricted
 - Strong identification
 - Audit logs



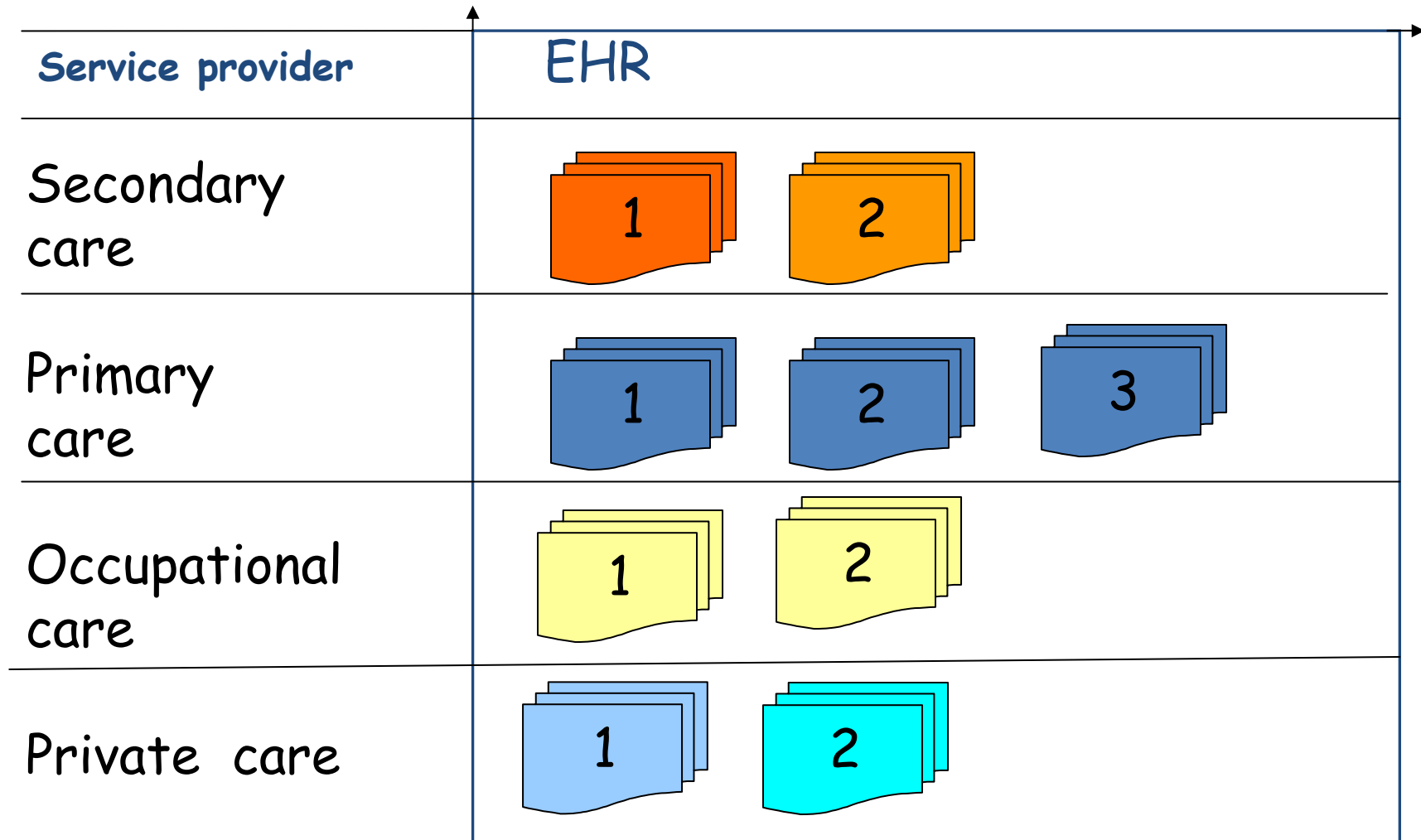
Patient's /person's view

- Consent
- Opt-out
- Audit- logs
- Access to disclose audit logs

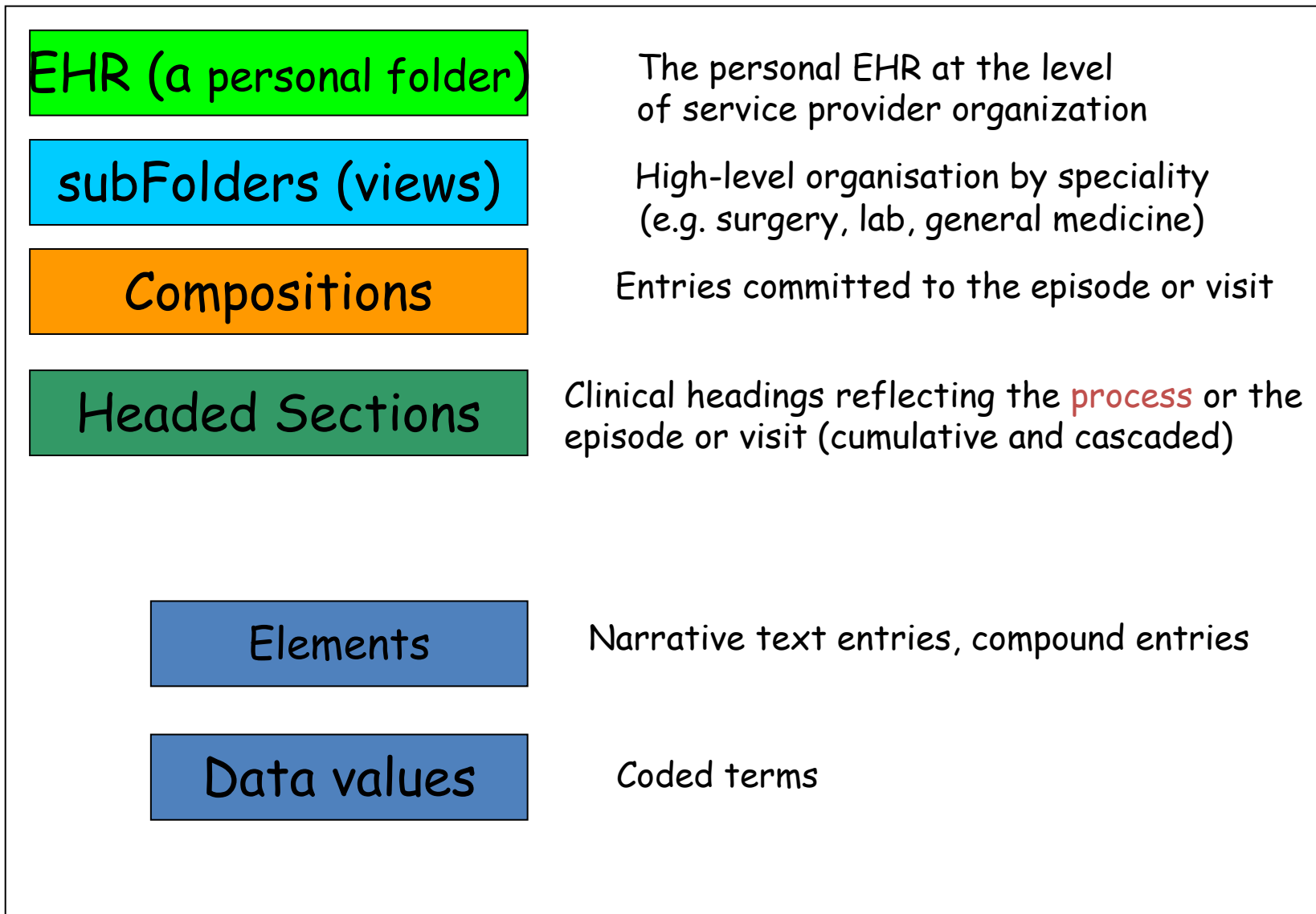
Basic features of the Finnish EHR

- An EHR is lifelong personal EHR at the level a of single service provider organisation.
- Any person or patient can have many separate organisation specific EHRs.
- There are only service provider level summaries available.
Finland there does not exist any organisations or persons having the responsibility to create a longitudinal patient summary.
- The EHR does not contain any specific security information or security related metadata

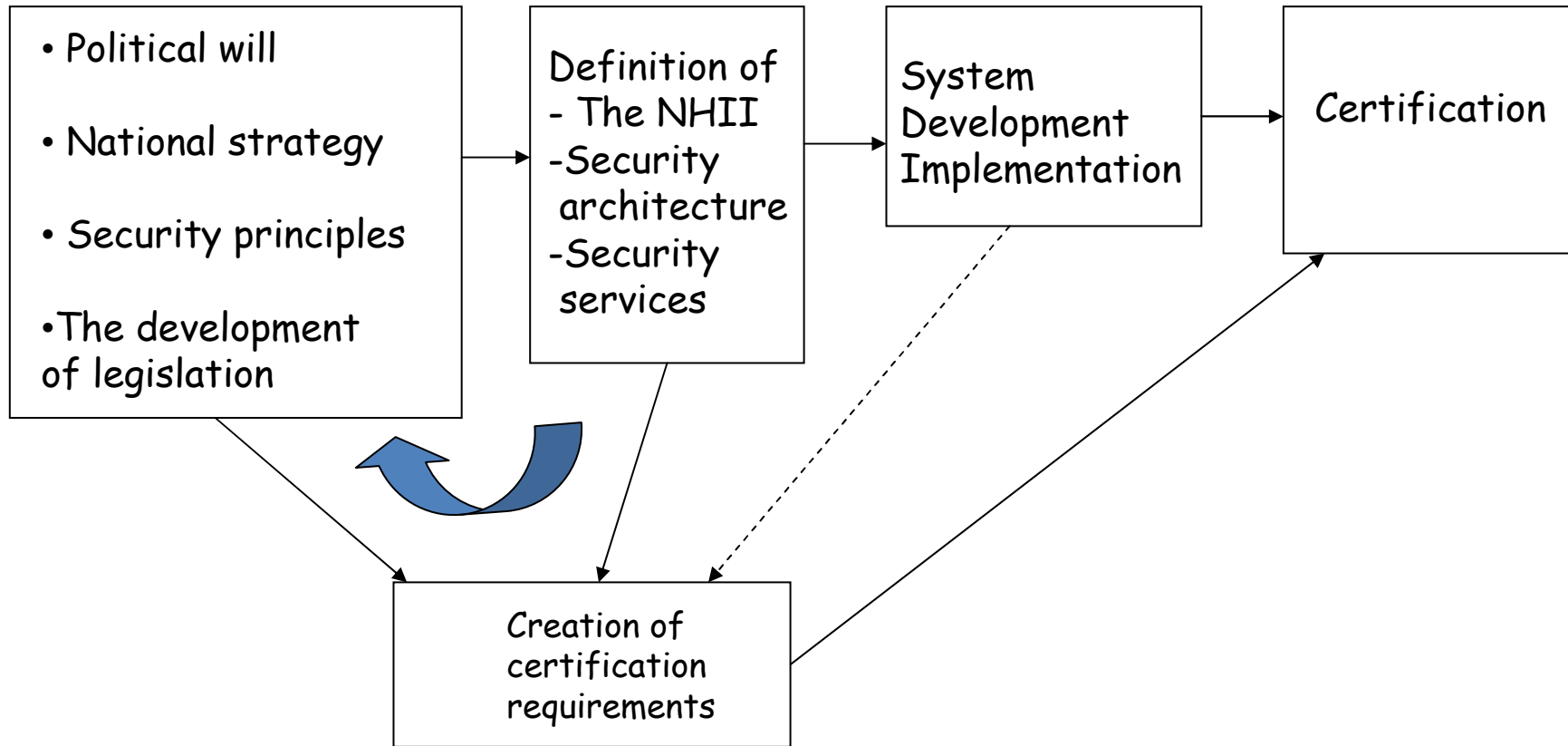
Horizontal and vertical views to the Finnish EHR architecture



The EHR structure an EHR



The roadmap to trusted sharing of the EHRs



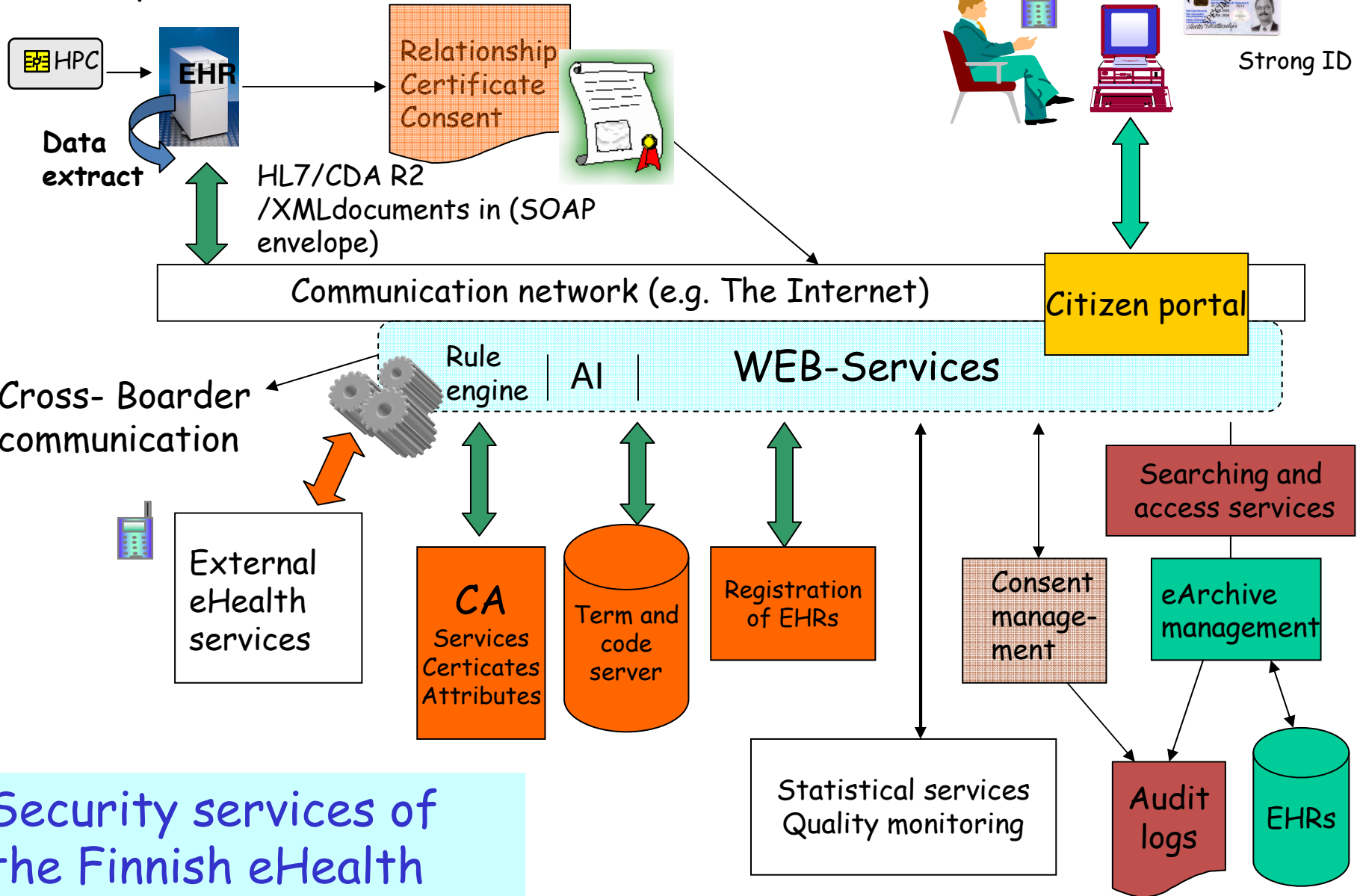
The Finnish NHII, its security architecture, functions and services

Legacy level
Security services

Citizen patient



Strong ID



Security services of
the Finnish eHealth
Infrastructure

The Finnish NHII includes four interconnected security domains

1. Security services the health care provider's EHR-system must provide (The legacy domain):

- Identification of patients and employees. Employees are identified using CA services and health smart health professional cards
- Local privilege management and access control service using RBAC
- The creation and updating of patients' consents and opt-out profiles
- e-signing EHRs using personal or organisational e-signatures
- Creation of care relationship certificates
- Creation of local audit trails

2. Communication domain

- Security is based on contracts between teleoperators, the service provider and national eArchive.
- Signed documents are transferred in SOAP envelopes.
- In the case of the Internet documents are also encrypted.

3. National security services (National domain)

- Certification services for regulated health professionals and entities
- Registration services for EHRs
- Consent management and distribution services
- Creation of disclose logs of EHRs
- Secure eArchiving services based on ISO TS 21457 principles
- Identification and certification services for citizens using the Internet (e.g. strong identification using smart citizen card)

4. Personal security domain

- Strong identification is mandatory for any access to own EHRs stored in the eArchive, and also for the access to EHR disclose logs.

Remaining risks and challenges

- The availability and usability of EHRs is a critical success factor. The eAchieve should offer intelligent browsing services, and disclose results via the network rapidly (in seconds). The practical service level of the eArchive and centralised consent management service are unknown.
- The creation of HL7CDA documents from local EHRs documents by legacy systems requires semantic mappings. This can cause risks for the usability of information.
- HL7CDA documents are not originally developed for a for secure long term archiving of EHRs. It is not proven if the use of them is the correct solution.
- Certification the trustfulness of the NHII is not done. Basic security and interoperability requirements has been published autumn 2008, but the certification process is still in progress.
- It is unclear what level of non-repudiation of events is needed and which events should be audited.

- There is still ongoing discussion of the consent model physicians will accept
- There is increasing pressure for secondary use of archived EHRs (e.g. for different public purposes, monitoring, profiling, proactive prevention and research). Legislation regulating the secondary use can change in 2-3 years.
- In the future it is necessary the whole NHII uses policy based access and EHR disclose control method, but service providers, the eArchive and software vendor are not familiar with model.
- The structure of present EHR does not support security and privacy protection. Therefore a new EHR structure is needed.

Summary: Security services of used in the Finnish NHII

- Common national security and privacy protection principles and rules
- PKI based health professional identification and certification services
- Role based privilege management and access control at legacy level
- PKI based certification of service provider organisations
- Documents are signed by the professional responsible for care using HPC
- CDA documents are e-signed and transferred in SOAP envelopes
- Complete auditing of events
- The eArchive is using rule based disclose control services for EHRs (Patient's consent/opt-out, purpose and patient-doctor relationship and rules derived from legislation are used to enable the disclose

Thank you for listening !



pekka.ruotsalainen@thl.fi