



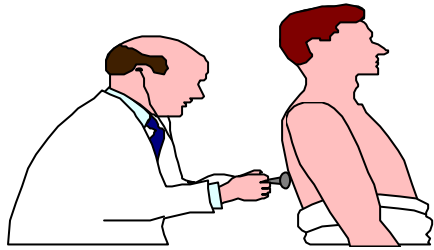
# Security standardization for Health Informatics

ITU-T eHealth conference  
Geneva 2003-05-23

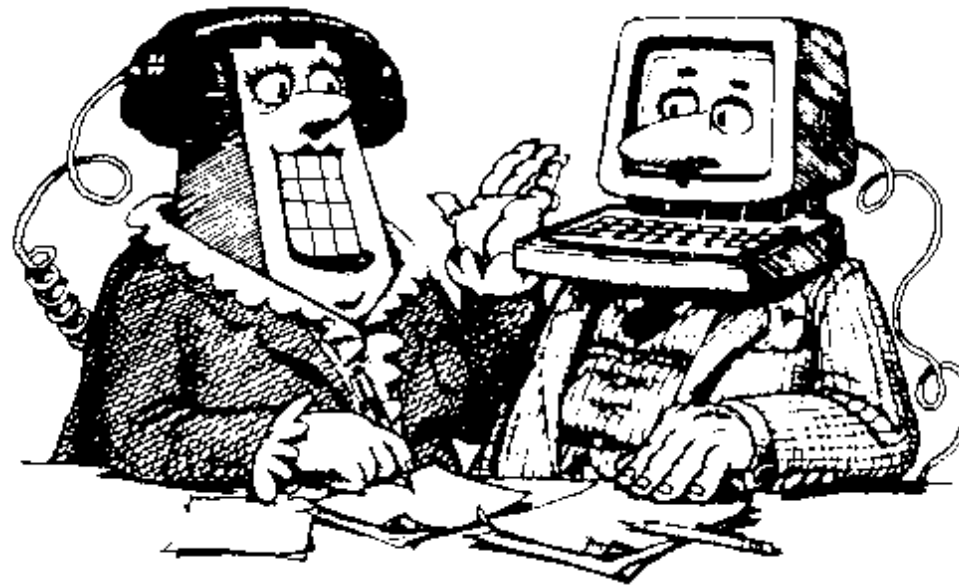
Dr Gunnar O. Klein

*convenor of ISO/TC 215/WG 4 "Security"*

**Karolinska Institutet  
&  
Swedish Standards Institute**  
*gunnar.klein@sis.se*



## ***Security - the forgotten requirement for interoperability***



**Can we really make the different systems talk to each other  
if we continue to ignore security ?**



# The core security requirements for e-Health

## ➤ A common way of secure user authentication

- Including a naming system to provide both national and cross-border uniqueness and linkage possibilities when required
- The standard method should provide user authentication with a common standardized technique for all possible systems

## ➤ A legally acceptable method for electronic signatures on digital documents

- Legislation in many countries demands signatures and lack of this has greatly slowed down e-health.

## ➤ Protecting confidentiality of communication

- Electronic mail through Internet
- Message handling systems (including SOAP web services)
- WWW access



## **Prerequisites for interoperable Electronic Signatures**

- **Technological solutions that allow security in open systems environments**
- **Standards for protocols and all components**
- **Pilot projects to gain experience**
- **Trusted Third Party Services**
- **National and International agreements to honour the TTP:s and methods developed**
- **Business decisions to implement the security services in all sorts of applications**
- **Responsible users**



# ISO/TC 215/WG 4

## Health Informatics Security

**Convenor:** Gunnar Klein, **Sweden**  
**Vice Convenor:** Ross Fraser, **Canada**  
**Secretary:** Nagaaki Ohyama, **Tokyo Institute of Technology**  
**Imaging Science and Engineering Laboratory**



## **A first set of Technical Specifications on Public Key Infrastructure approved 2001**

- ISO/TS 17090: Health informatics - Public key infrastructure -
  - Part 1: Framework and overview
  - Part 2: Certificate Profile
  - Part 3: Policy management of certification authority



## **ISO/TC 215/WG 4 work in progress**

- Health informatics – Directory services for security, communications and identification of professionals and patients
- Project leader: Lori Reed-Forquet, USA
  - Supporting the use of certificates in a public key infrastructure for a variety of security services including access control
  - Also providing other services for identification and finding communication meta-information



## Health informatics - Guidelines on data protection to facilitate trans-border flow of personal health information

Project leaders: Ray Rogers (UK),  
Brendan Seaton (Canada)

Status: Draft international standard





**Health informatics - Security requirements for archiving and backup –  
Part 1: Archiving of health records**

Project leader: Pekka Routsalainen, Finland  
Type of Document: Technical Specification

**Health informatics - Security requirements for archiving and backup –  
Part 2: Guidelines for backup**

Project leader: Ernst Leitgeb  
Type of Document: Technical Report



## Health informatics – Privilege management and access control

Project leaders: Bernd Blobel, Germany  
and Ragnar Nordberg, Sweden

Joint work with CEN

Target: Technical Specification



## **Health Informatics - Framework for health information security**

Type of Document: Technical Report

### **Health informatics - Functional and structural roles**

Type of Document: Technical Specification

### **Guidelines for Security management in health using ISO 17799**

Type of Document: Technical Specification

# **CEN/TC 251/Working Group III: Security, Safety and Quality**

- **Guidelines for management of security for health**
- **Detailed protocols for various core security services based on inter-sector standards.**
- **Data protection in the context of the EU data protection directive, particularly for communication outside of Europe.**
- **Access control policy bridging and systems for Anonymisation.**

# CEN publications for security

- ENV 13608:
- Health Informatics - Security for Healthcare Communication
  - Part 1. Concepts and Terminology
  - Part 2. Data Object Security
  - Part 3. Data Channel Security

These build on work from IETF (Internet Engineering Task Force)

- Health Informatics - Secure user identification for healthcare - management and security of authentication by passwords - ENV 12251
- Health Informatics - Secure User Identification for Healthcare Strong Authentication using Microprocessor Cards ENV 13729

# **CEN publications for security**

## **ENV 12924**

**Health Informatics - Security categorisation and protection for healthcare**

**Health Informatics – International transfer of personal health data covered by the EU data protection directive- High level security policy**

**Health informatics – Guidance on handling personal health data in international applications in the context of the EU data protection directive**

## **Some new work of CEN**

**Health informatics - Anonymisation user requirements**

**Health informatics – Electronic health record communication – Security requirements**