A Secure Extranet supporting Medical Data Exchange between Organisations

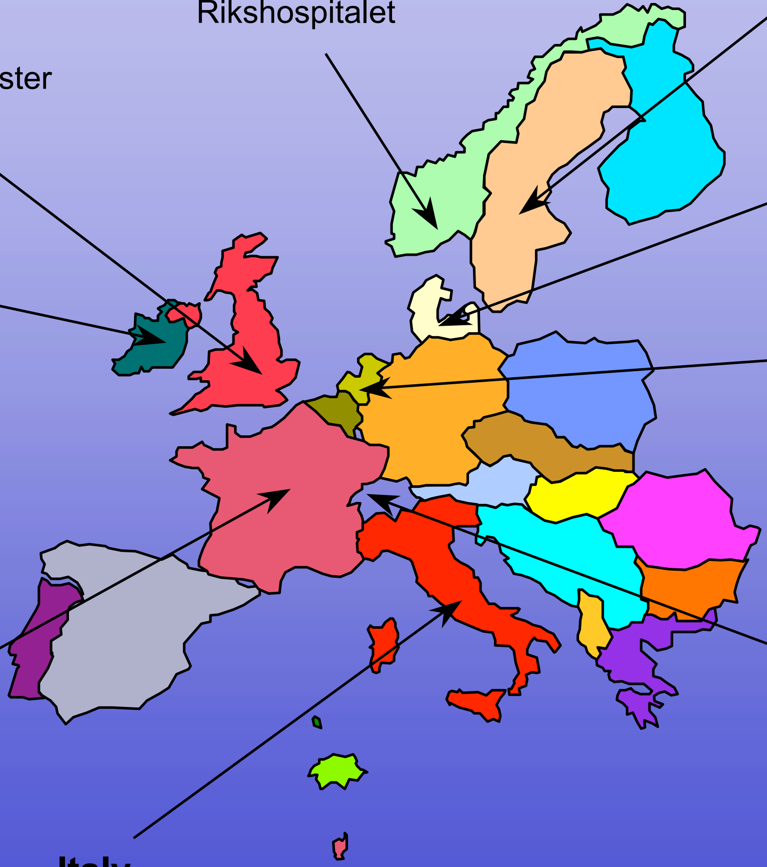
SWITCH AAI Workshop
Gerzensee, November 20-21, 2000

Dr. Sc. Stéphane Spahni
Health on the Net Foundation &
Medical Informatics Division / University Hospitals of Geneva

The "Synex" European Project

- Promote shared and distributed healthcare records
- Provide tools to share information across large organisation-wide networks and between organisations
- *Produce a set of products that are generic, modular and re-usable*
- *Define industry-led standards*

Synex Partners



Norway
Siemens Nixdorf
Sentralsykehuset Akerhus
Rikshospitalet

Sweden
TietoEnator AB
Uppsala University

United Kingdom
University College London
Victoria University Manchester

Denmark
Danish Institute for Health and
Nursing Research

Ireland
St James's Hospital
Trinity College Dublin
Decision Support Systems
Dublin Institute of Technology

Netherlands
Erasmus University Rotterdam
St Franciscus Gasthuis Rotterdam
St Clara Hospital Rotterdam
University Hospita Dijkzigt Rotterdam
Katholieke Universiteit Nijmegen

Switzerland
Geneva University Hospitals
Nice Computing
IBEX
FMH / Arpage
AMG
IBM
Swisscom

France
HEGP/Broussais Hospital

Italy
GESI
UCSC - Policlinico A Gemelli

Geneva Demonstrator

- Secured Extranet between the Hospitals and the GPs

➢ Access to patient records

➢ Electronic transfer of documents from the hospitals to the GPs (e.g. discharge letter)

Security Requirements

- Needs for:
  - Encryption of the transmission
  - Authentication of the users
  - Closed users groups
  - User profiles
  - Client software independence

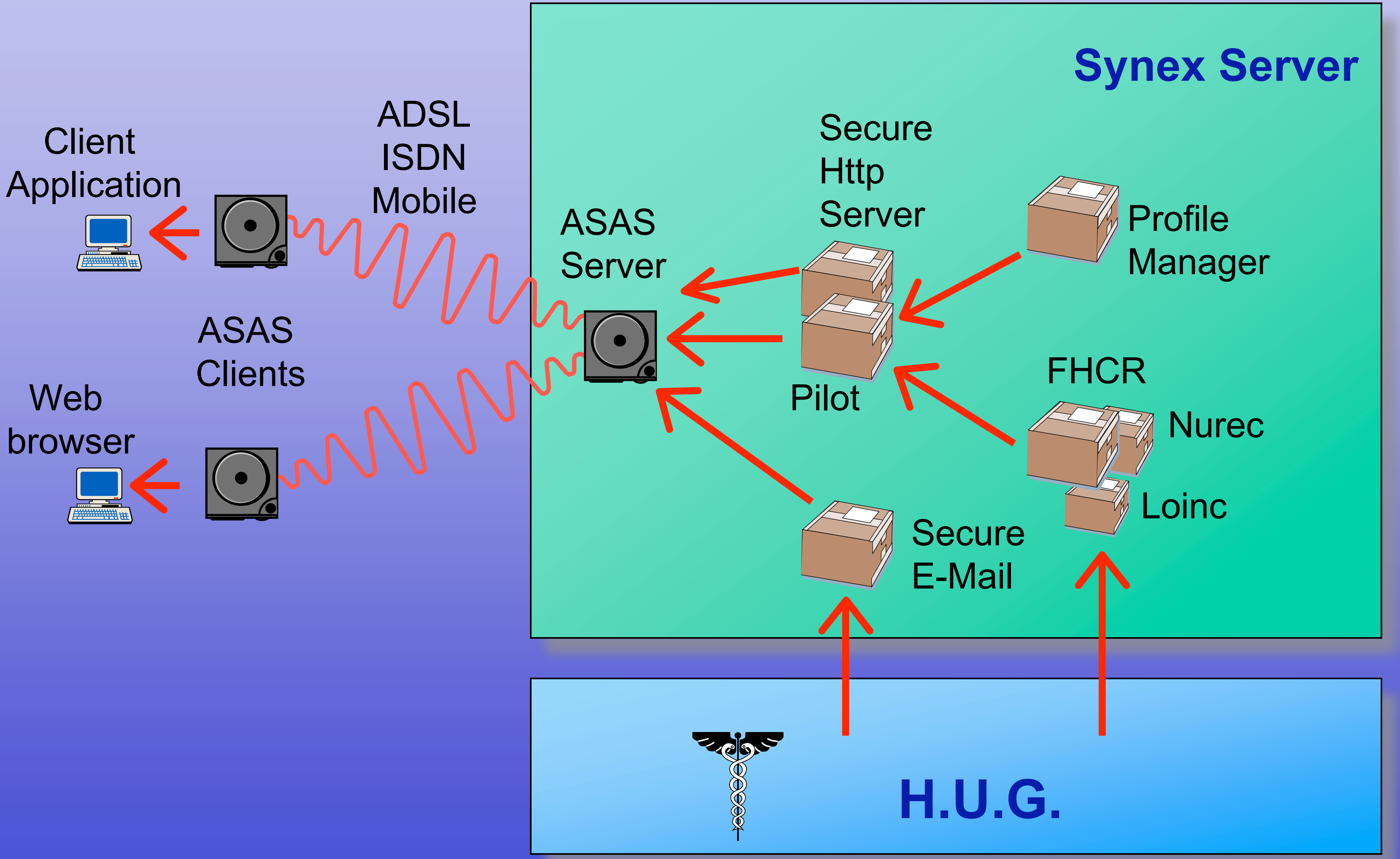
➢ Public-Key Infrastructure

➢ Profile Management

PKI Infrastructure

- Based on the ASAS Security Toolkit
- Private Certification Authority
- Implementation using the main standards: RSA, 3-DES, X.509 certificates, SSL
- Supports HTTPS, S/MIME

Communication Infrastructure



Benefits

- Private PKI Infrastructure available and recognized at a national level (FMH)
- Infrastructure based on existing standards
- Independence against the mail agent
- Available for any single-socket application

Known problems

- Multiple (incompatible) platforms exist
  - Need for coordination & harmonization (e.g. X.509 attributes)
  - Not easy for the user (*n* PKI infrastructures)
- CA not recognized automatically by common software (e.g. Messenger, Outlook)
- Exploitation still in preliminary phase
  - Organisational tasks (e.g. renewal of certificates)
  - Distributed authentication servers

Using a general purpose PKI ?

- Advantages:
  - Faster kick-off
  - Existing experience
  - One certificate for many different uses
- Disadvantages:
  - Does not solve the access control problem (Closed users groups)
  - Control of the CA (notion of « community »)