PUBLIC RESEARCH CENTRE HENRI TUDOR
SANTEC - Healthcare Technologies

WS 5 - Healthcare Professional

Identification, Authentication and Authorization

Uwe Roth

21. September 2011 - 14:15-15:45
29JFK, Salle Saarbrücken

www.tudor.lu

Need for Authentication

In the Context of eHealth

Concepts

- **Identification**
  I know who you claim to be
  John Doe
- **Authentication**
  I know/proved who you are
  John Doe, General Practitioner
- **Authorization**
  I know what you are allowed to do
  Access to File X245-PQ

Authentication Needed

- Authorization
  to access services and data
- Determination of
  the origin of data and
  the use of services

Who Needs To Be Authenticated

- **Individuals**
  Health professionals
- **Institutions**
  Hospitals, laboratories, ...

Known After Authentication

- **Identity**
  - The health professional as a individual
  - The institution
- **Structural and Functional Roles**
  - Structural Role: Professional category
    Professions and specializations of the health professional
  - Functional Role:
    Family doctor, medical consultant, patient, ...
  - Areas of activity of the institution
- **Working Context**
  - Relationships between health professional and institution

Granting Access To Services and Data: Policies

- **Functional and structural roles:**
  Role based access control lists
- **Patient consent**
- **Working context**
  optional

Resources Needed

To Authenticate
Health Professionals and Institutions

Register

- Official data for defining structural roles
- Dispose a clear identification number

Potential Sources

- **Ministry of Health / Health portal directory:** Health care professionals, hospitals, labs, pharmacies,…
- **Ministry for Family and Integration:** Long term care, homecare
- **Caisse nationale de Santé:** Complementary data

Will be analyzed

Data in the Register
Health Professionals

- **Name, surname**
- **Title**
- **Roles**
  Professions, specializations, activities
- **ID numbers**
- **Working place**
  Need for synchronization with local directories
- **Address information**
- **Contact information:**
  Phones, fax, e-mail
- **Public for the healthcare sector**
  Example: Searching for ID of recipients for documents

Unique Identification Number

To Identify Health Professionals and Institution

Unique Identification Number

- **No specific identification number is issued by official sources for healthcare professionals and institutions when authorizing their activity**
- **Candidates**
  - Matricule
  - CNS number
  - ISO Object identifier OID

Matricule

- **Pro:**
  - Quite stable (with some exceptions)
- **Con:**
  - Revealing personal information: age, sex
  - Acceptance problem

CNS-Number

- **Pro:**
  - Already used as ID number
  - Acceptance
- **Con:**
  - More than one CNS number possible per health professional or institution (different working place, association,…)
    - To limit to the individual CNS number for a professional to a clear individual identification
    - How to deal with different CNS number per institution?
- **Need to check how stable the number is in time**

ISO Object Identifier OID

- **Pro:**
  - Can be defined per user unit and controlled by the Agency if it registers an OID
    (own register or in other existing register)
  - Stable and worldwide unique
  - OIDs are needed as well for CDA templates, local catalogues and dictionaries (HL7 requirement)
- **Con:**
  - Not used so far in the Luxembourgish healthcare sector
  - Change management + acceptance problem
  - Number is not handy (e.g. 1.3.6.1.4.1.32703.1.2.1.1)

How to Authenticate

Individuals and Institutions

Ways of Authentication

- **Something you know - Knowledge/Secret:**
  - Login/Password
  - PIN
- **Something you have - Ownership:**
  - Smartcard
  - Token
  - Phone
- **Something you are - Biometric Property:**
  - Fingerprint
  - Retina

Strong Authentication

- **Two factor authentication**
- **Two of the three:**
  - Know + Have:
    e.g. Smartcard + PIN
  - Know + Are:
    e.g. Fingerprint + Password

Authentication and Cryptography

- **Smartcard/Signaturcard**
  - Private key is only stored on card public key stored on server
  - User sends identity
  - Server sends random
  - PIN used to enable private key
  - Card encrypts random number with private key
  - Result is send to server
  - Server decrypts with public key
  - If number is initial number, authenticity is proven
- **Token**
  - Token produces pseudo-random number each minute
  - User reads number and sends it to server + Identity + PIN
  - Server is able to produce same series of numbers on base of identity
  - If at the same minute, correct number and PIN are used, user is authenticated

Types of Cards
LuxTrust

- Identifies persons, not only doctors
- Persons might have several cards
- Card must be somehow registered in the system
  - Online registration
  - Application form
  - One-time password
- No additional information stored on card
- Link to role must be managed in special server
- Lifecycle (production, withdraw, renewal, ...) exists
- In-out cycles of card in card reader only 1000 times guaranteed
- Hygiene might be a problem
- Can be used for signing of documents
- Backup card needed in case of broken, stolen, forgotten card

Types of Cards
Special Health Professional Cards

- **Can be customized, e.g. picture of doctor on card**
- **Roles as meta data on card possible**
- **Renewal of card if change of meta data**
- **Issuer of card must be identified**
- **Lifecycle must be setup**
- **Contactless cards possible**
  - disposable cover to ensure hygiene requirements
  - extended durability
  - usability
- **Backup card needed in case of broken, stolen, forgotten card**
- **Can be used for signing of documents**
- **Compliant with HPRO Card specification (surface layout)**

Types of Cards
Tokens

- Only for authentication
- No signing of documents possible

Authenticity

Of Documents

Authenticity

- **Prove, that someone was the source of a document**
- **Electronic signature of the document**
- **Signature of the creator (= doctor)**
  - Requires manual intervention
- **Signature of the institution**
  - Creator information as meta-data
  - Can be performed automated
  - Creator-information might be faked

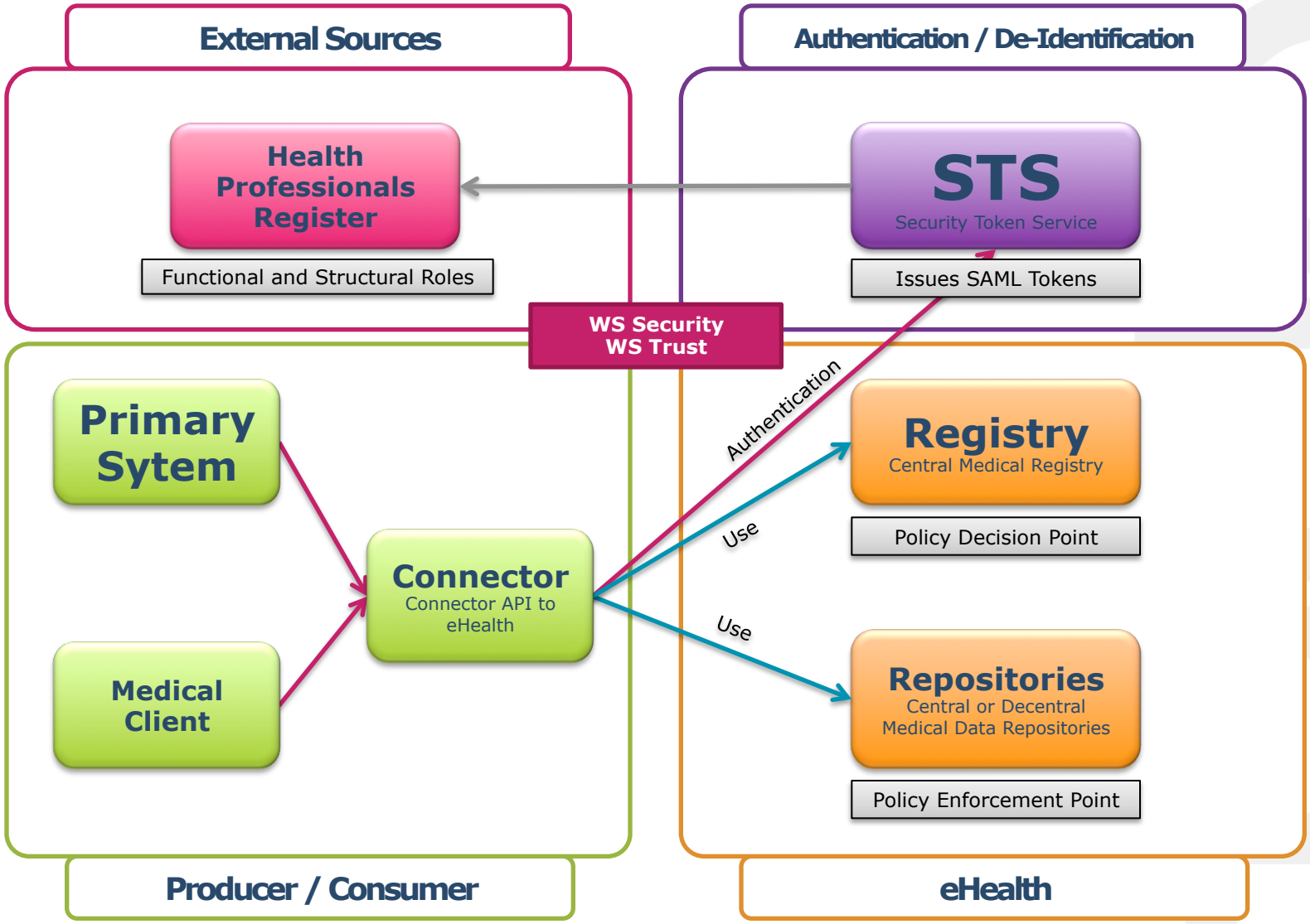
Security Requirements

In the eHealth Context

Security Requirements

- **Access to data only after strong/two-factor authentication**
  - The medical life of patients needs to be protected from unauthorized access
  - Encrypted and de-identified storage of medical data in the eHealth platform would be useless, if access control is not enforced
- **Storage of data only signed to prove origin**
  - Fake data entered by non-existing doctors might lead to wrong treatment
- **Communication between Institution and eHealth Infrastructure**
  - Via Connector API / Connector
  - WS Security / WS Trust

Overview


External Sources
Authentication / De-Identification
Health Professionals Register
Functional and Structural Roles
STS
Security Token Service
Issues SAML Tokens
WS Security
WS Trust
Primary Sytem
Medical Client
Connector
Connector API to eHealth
Authentication
Use
Use
Registry
Central Medical Registry
Policy Decision Point
Repositories
Central or Decentral Medical Data Repositories
Policy Enforcement Point
Producer / Consumer
eHealth

WS Security / WS Trust

- **Health Professional Register**
  - Manages all health professionals
  - Manages functional and structural roles of health professionals
- **STS Security Token Service**
  - User/institution needs to authenticate at STS
  - STS issues SAML to token with all role information
- **Registry**
  - Policy decision point
  - Takes decision about permission to access data on base of SAML token and policies
  - SAML Token will be enriched with XACML
- **Repository**
  - Policy enforcement point
  - Document will be delivered or not on base of SAML Token

Options to be Discussed

Authentication of Users and Institutions Towards the eHealth Platform and Signature of Documents

Authentication and Signature of Institutions

- **Authentication of institution and signing of submission-set is done at the connector**
- **Institution might also sign document and guarantees that creator-information is correct:** First pragmatic and easy to start solution

Authentication and Signature of Institutions

- **Password protected soft certificate / SSL certificate**
  - Someone needs to enter password if system crashes (24/7)
  - Certificate useless if copied
  - Quick and easy solution
- **Hardware Security Module HSM**
  - Protection against software based and physical attacks and non-authorized used
  - Potentially faster as special optimized hardware used to implement cryptographic functions e.g. signing
  - Certified hardware available
  - Recommended for long-term solution

Authentication and Signature of Individuals

- **User authenticates via strong / two-factor authentication to access data or services**
- **User needs to authenticate individually**
  as in private practice
- **No aggregative or department account**
- **User signs documents and submission sets individually**
  in best case

Authentication and Signature of Individuals

- **User authenticates directly towards the eHealth platform and signs documents, e.g. via contactless smartcards**
  - Requires additional infrastructure in the institution/office
  - Processes must be adapted
- **User authenticates as usual in in-house system**
  - Institution must guarantee authenticity of user
  - Not each institution uses two-factor authentication today: not sufficient
  - Fake doctors might be created in the in-house system
  - How to pass in-house authentication to eHealth platform, e.g. via in-house STS?

Open Discussion

Comments, Remarks, Suggestions

uwe.roth@tudor.lu