SAML and XACML in Swedish healthcare

Ludwig Seitz
Axiomatics AB, Sweden

Background

- BIF: Base Services for Information Provisioning
  - Tender-bidding initiated by the Swedish Medical Care Advice Service
  - Goal: common IT-solutions for electronic patient records
    - e.g. common choice of technologies for future security services
    - Based on standards

Background ctd

- Goals for BIF services
  - Reliable access for authorised personnel
  - Protection against unauthorised disclosure
  - Integrity protection
  - Audit trail supporting non-repudiation

Even more Background

- Required services
  - Authentication and Authorisation
  - Care relation certification
  - Patient consent certification
  - Patient-data release
  - Secure patient context
  - Logging and Log analysis
  - Notifications

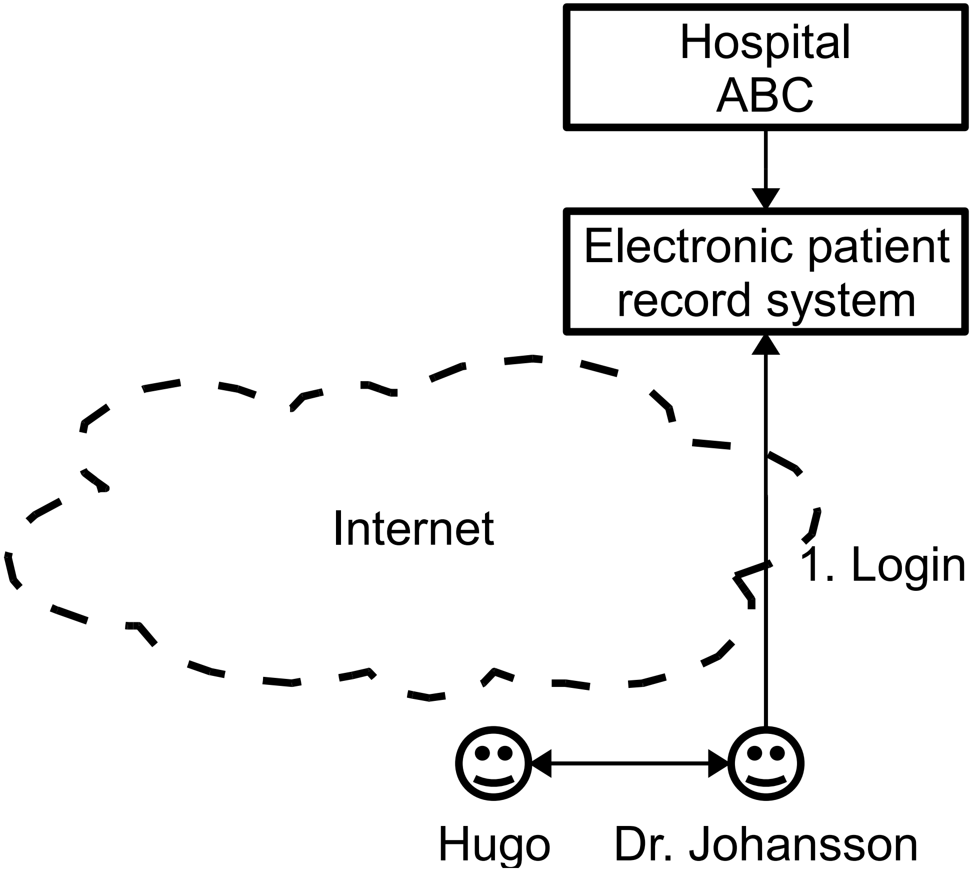
Some specific requirements

- Authentication
  - Use X.509 for authentication
  - Use SAML for identity federation
- Authorisation
  - Use XACML

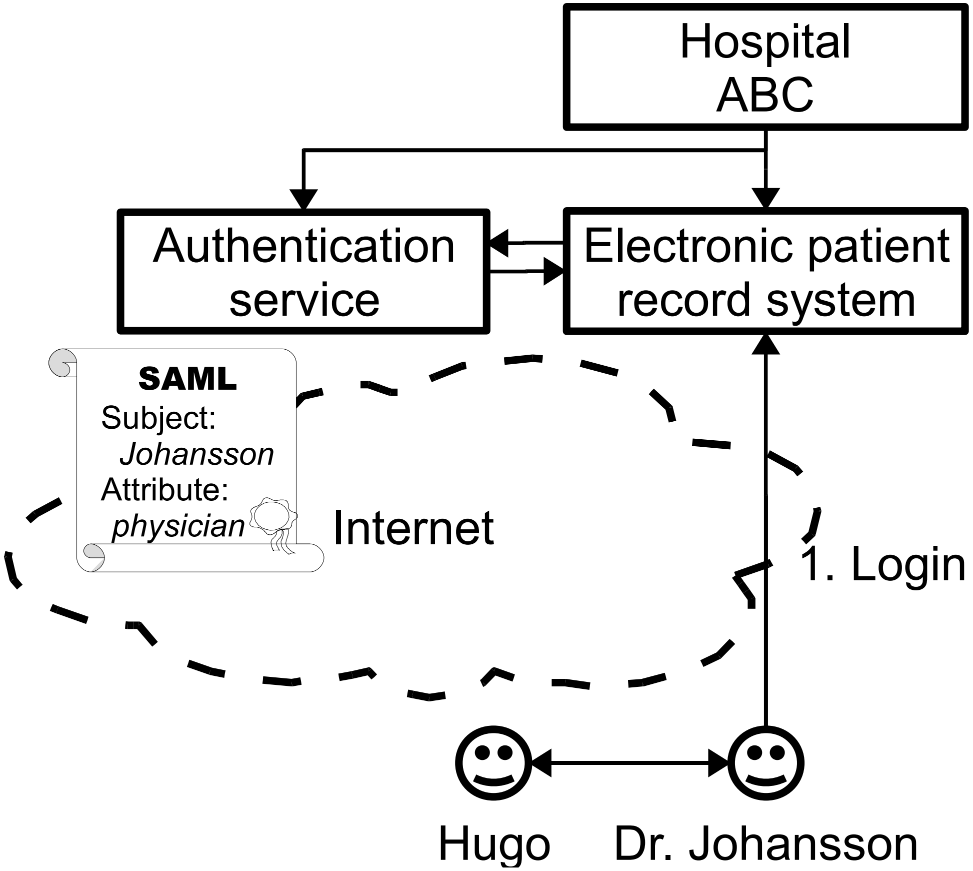
Overview - typical use-case

- Actors
  - Hospital *ABC,* provides electronic patient record system
  - *Dr. Johansson,* connected to ABC
  - *Hugo,* New patient
  - *Hospital XYZ ,* H.'s previous care centre
- Scenario
  - Transfer of electronic patient records

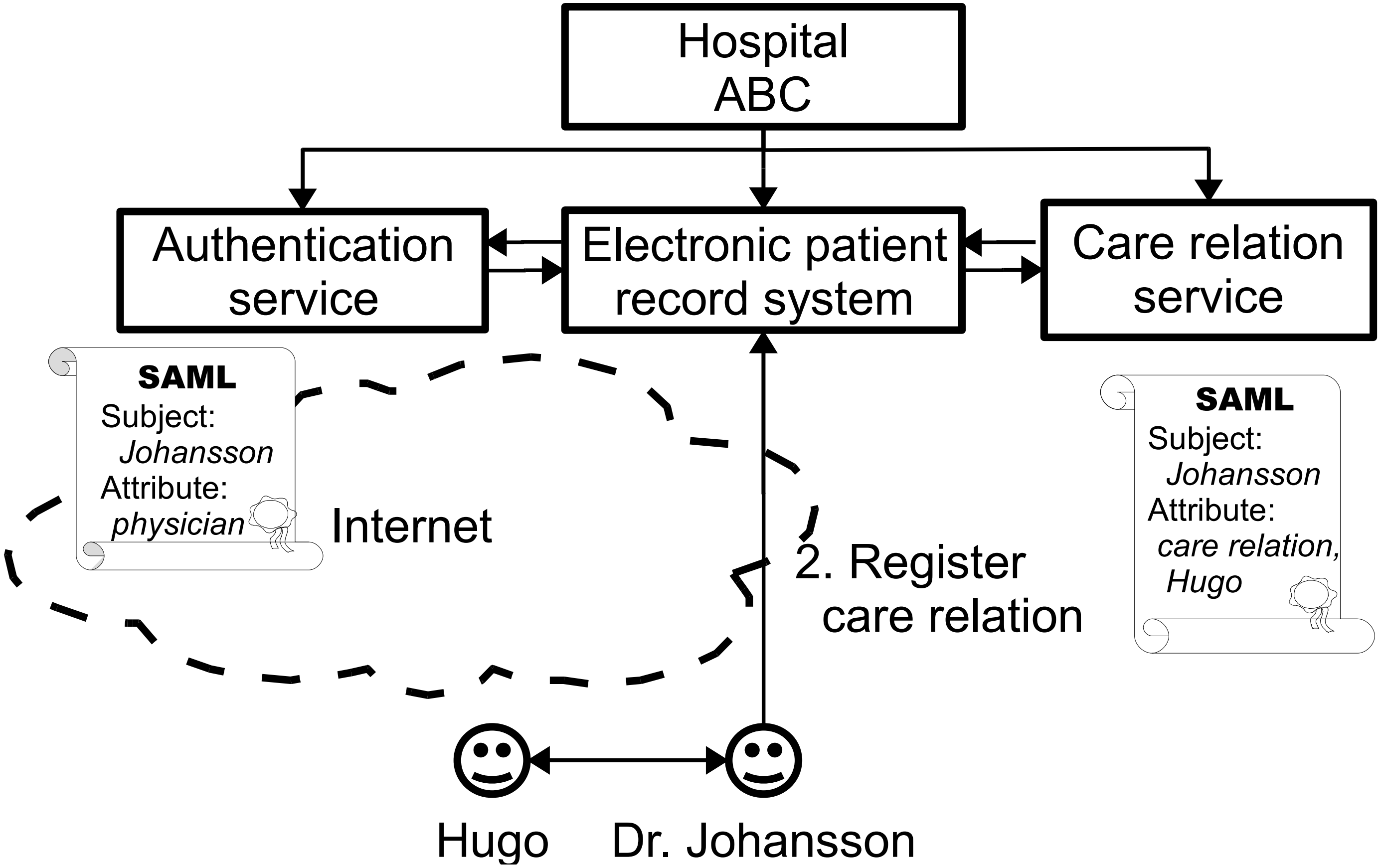
Typical use-case



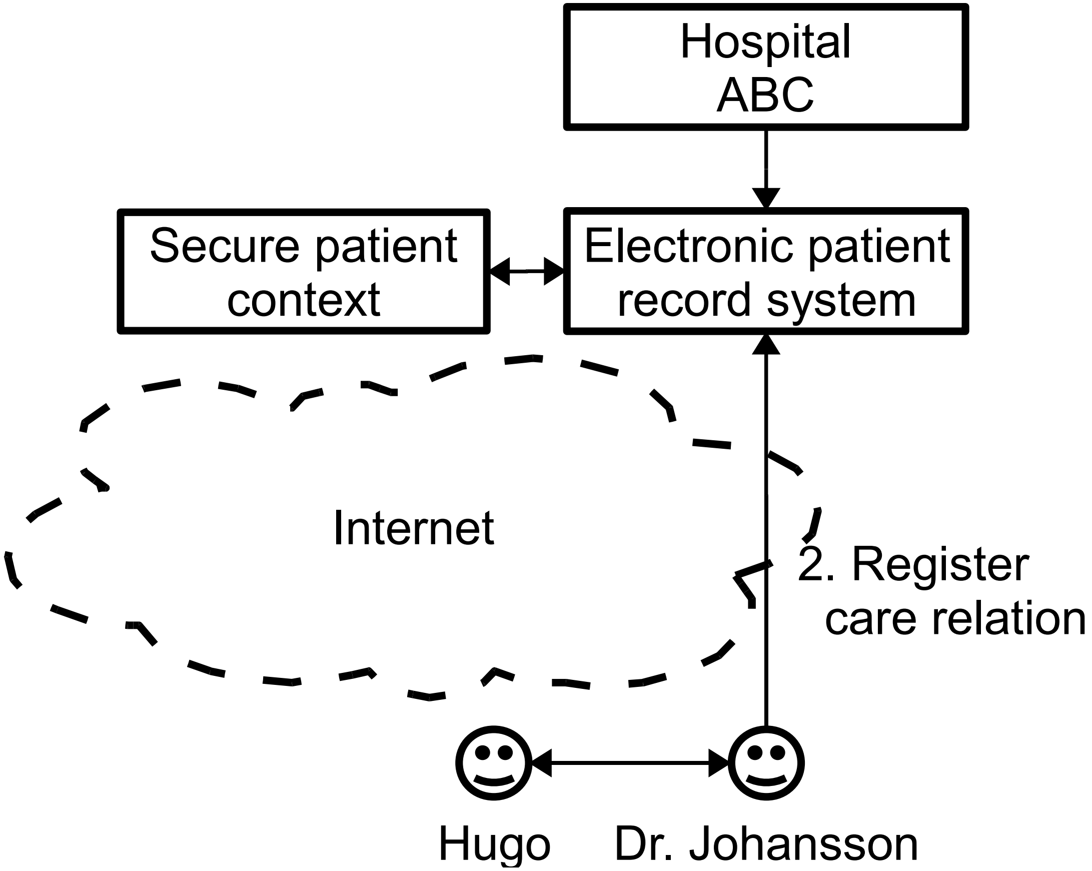
Typical use-case



Typical use-case



Typical use-case



Hospital ABC

Secure patient context

Electronic patient record system

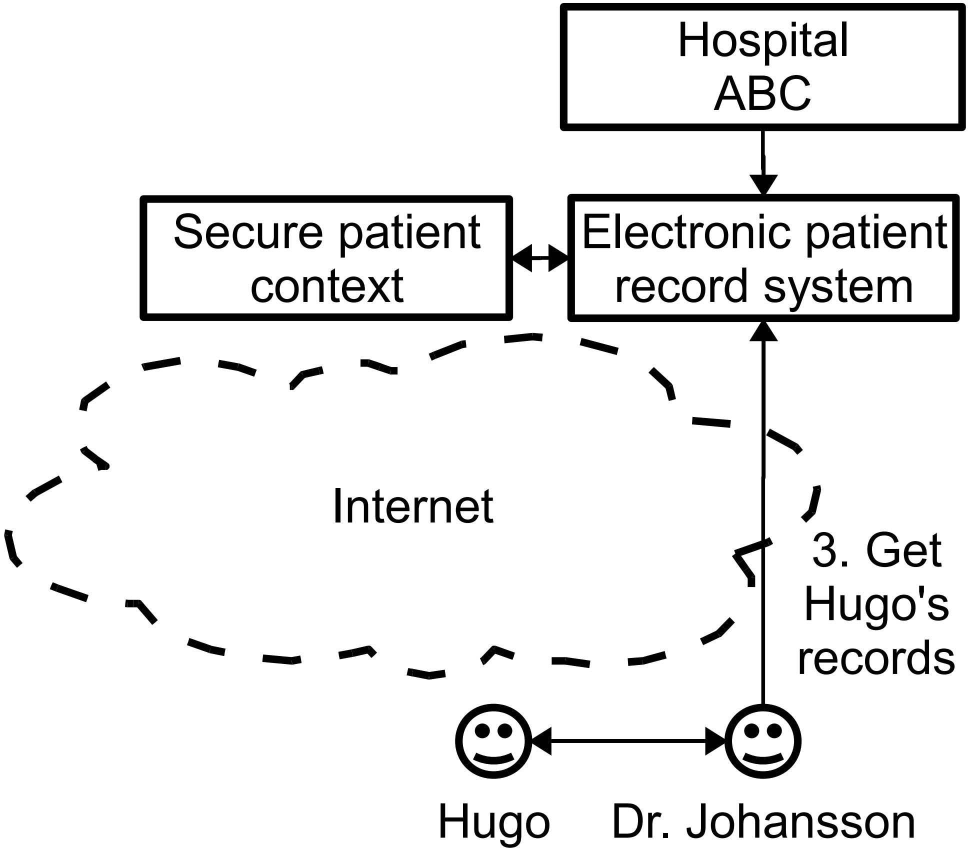
Internet

2. Register care relation

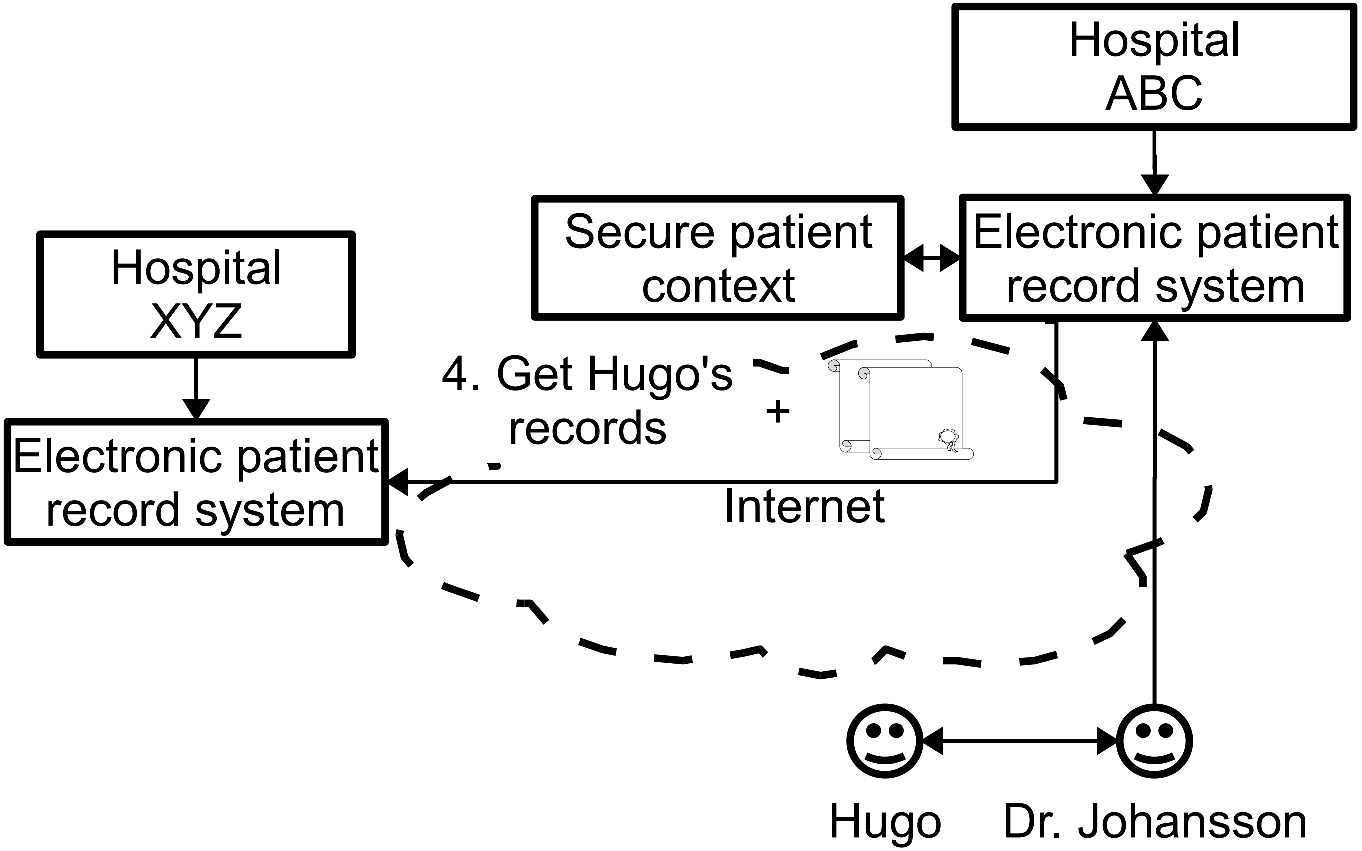
Hugo

Dr. Johansson

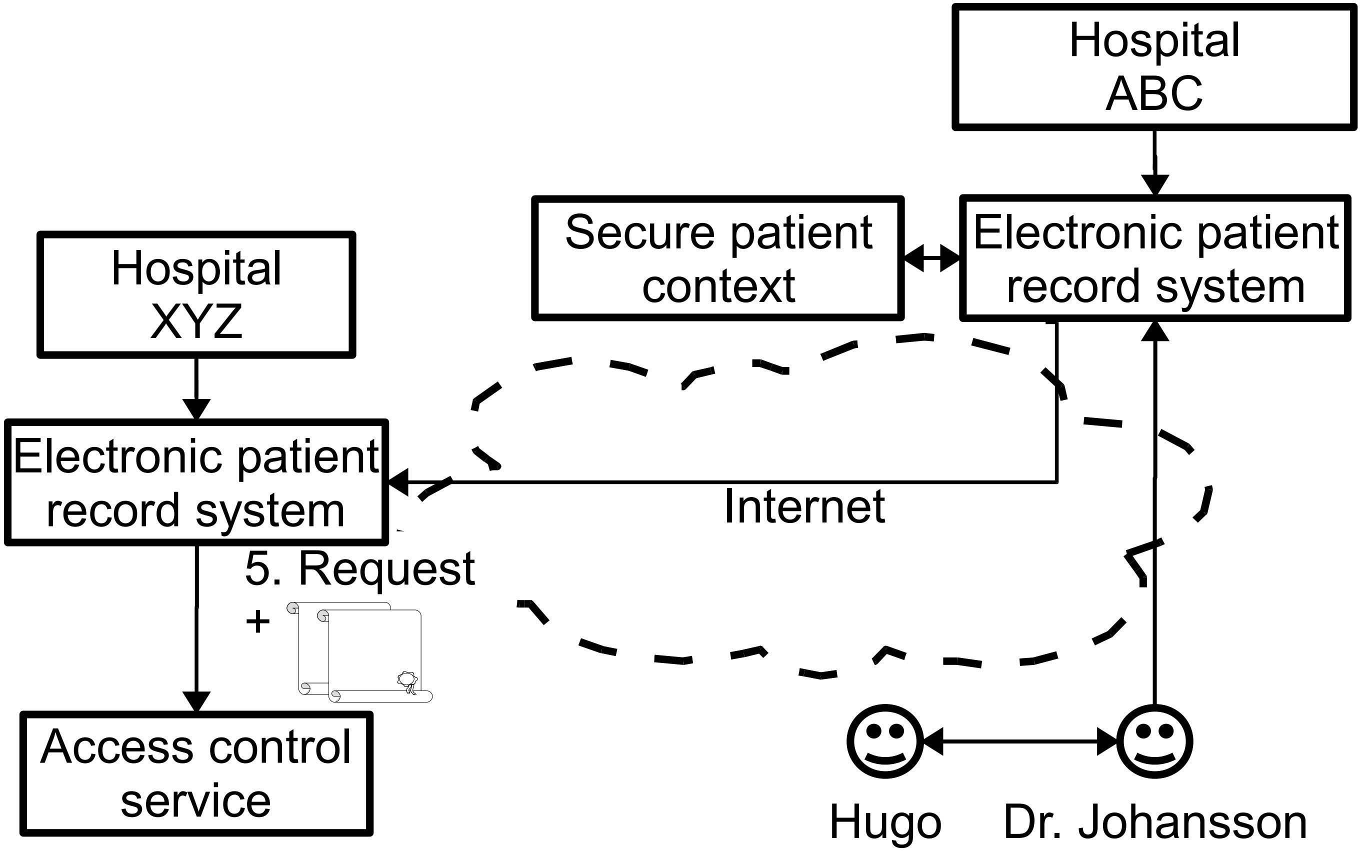
Typical use-case



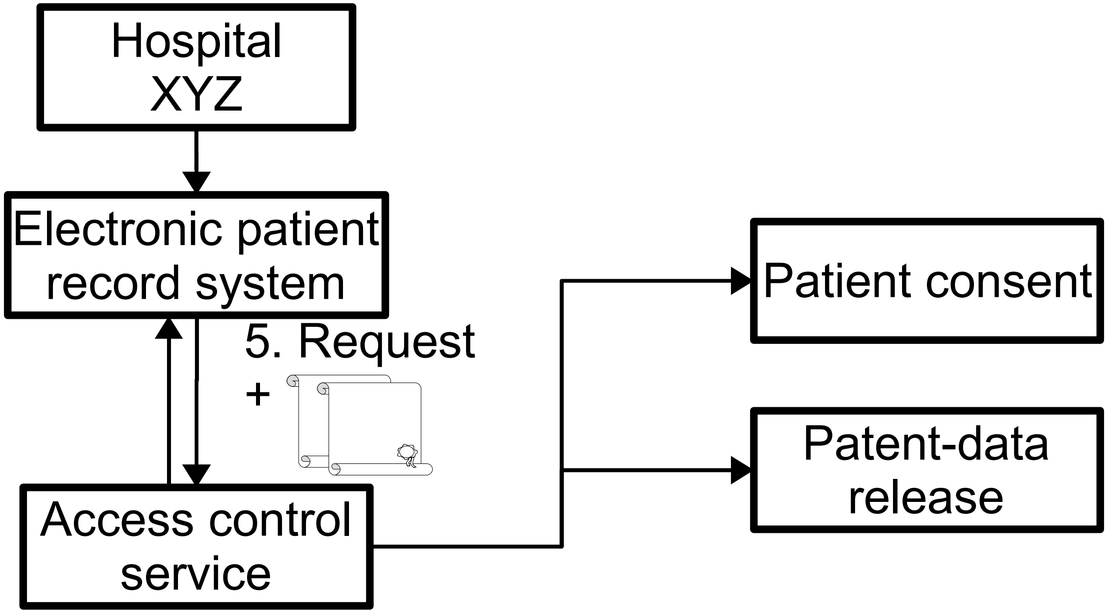
Typical use-case



Typical use-case



Typical use-case


Hospital XYZ
Electronic patient record system
5. Request
+
Access control service
Patient consent
Patent-data release