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
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

1. Login

Hospital
ABC

Electronic patient
record system

Internet

Hugo

Dr. Johansson

OASIS
Typical use-case

1. Login

Dr. Johansson

Hospital ABC

Electronic patient record system

Authentication service

Internet

Hugo

SAML
Subject: Johansson
Attribute: physician

1. Login

Dr. Johansson
Typical use-case

1. Internet
   Authentication service
   Electronic patient record system
   Care relation service

2. Register care relation
   Hugo
   Dr. Johansson

SAML
Subject: Johansson
Attribute: physician

SAML
Subject: Johansson
Attribute: care relation, Hugo

Hospital ABC
Typical use-case

2. Register care relation

Hospital ABC

Electronic patient record system

Secure patient context

Internet

Hugo

Dr. Johansson
Typical use-case

3. Get Hugo's records

Secure patient context

Electronic patient record system

Hospital ABC

Internet

Hugo

Dr. Johansson
Typical use-case

1. Hospital XYZ
2. Electronic patient record system
3. Secure patient context
4. Get Hugo's records
5. Internet

Hospital ABC
Electronic patient record system
Hugo
Dr. Johansson
**Typical use-case**

Hospital XYZ

Electronic patient record system

Access control service

5. Request

Hospital ABC

Secure patient context

Electronic patient record system

Internet

Hugo

Dr. Johansson
Typical use-case

Hospital
XYZ

Electronic patient record system

Access control service

5. Request
+

Patient consent

Patent-data release