BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

A Privacy-Aware Localization Service for Healthcare Environments

Thomas Scheffler

PETRA 2011: Privacy and Security in Pervasive e-Health and Assistive Environments Workshop (PSPAE)

Heraklion, Crete 25.-27. May 2011

Overview

- Motivation and Idea
  - Data Owner controlled privacy policies
  - KopAL System and Requirements
- Policy languages for localization data
- Conclusion and Outlook

Motivation and Idea

Data Privacy for Location Services

Privacy Definition:

"...the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others."

P. Ashley and G. Karjoth, 2003

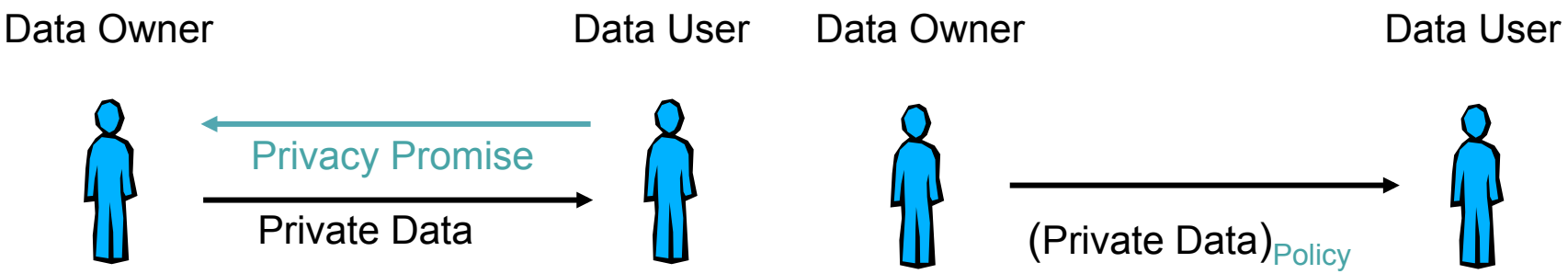
Controlling Data Access Policies

Data User controlled Policies

- The Data User specifies and publishes the access and use policy for private data.
- The Data Owner has to trust this policy and releases his/her data.

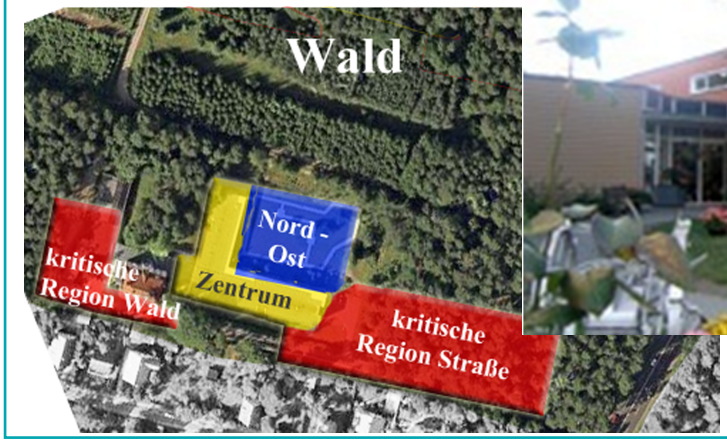
Data Owner controlled Policies

- The Data Owner specifies the access and use policy for data.
- The Data User enforces this policy.



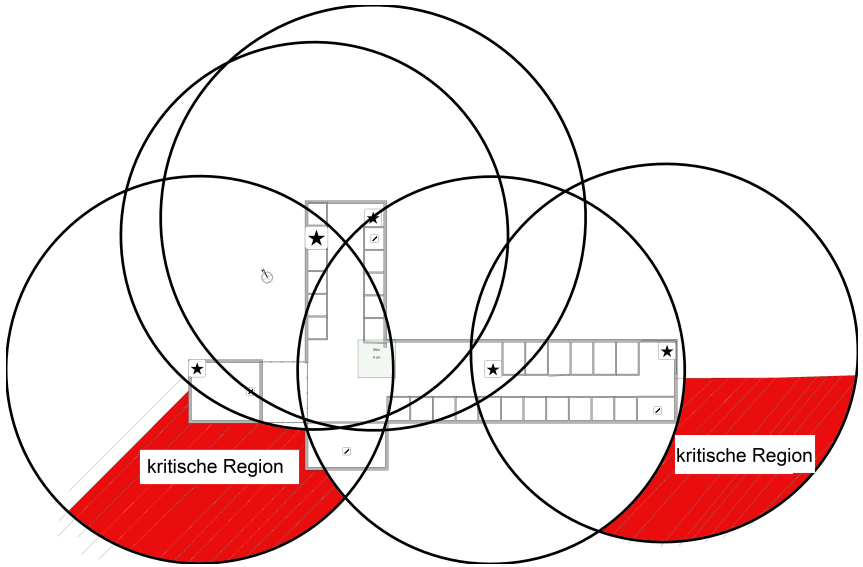
KopAL: Assistance for Patients with Dementia

- KopAL has been introduced by Sebastian Fudickar (PETRA2011, Workshop 1)
  - Electronic assistance for patients suffering from dementia
  - Emergency call function
  - Speech-based appointment reminder
  - Developed at Potsdam University, Germany
    http://www.cs.uni-potsdam.de/bs/research/al/index.html



KopAL: Assistance for Patients with Dementia

- Localization function in KopAL:
  - Localization of patients that have lost orientation
  - Notification of nursing staff about dangerous patient movement
  - Localization of lost or misplaced devices (requested by staff)



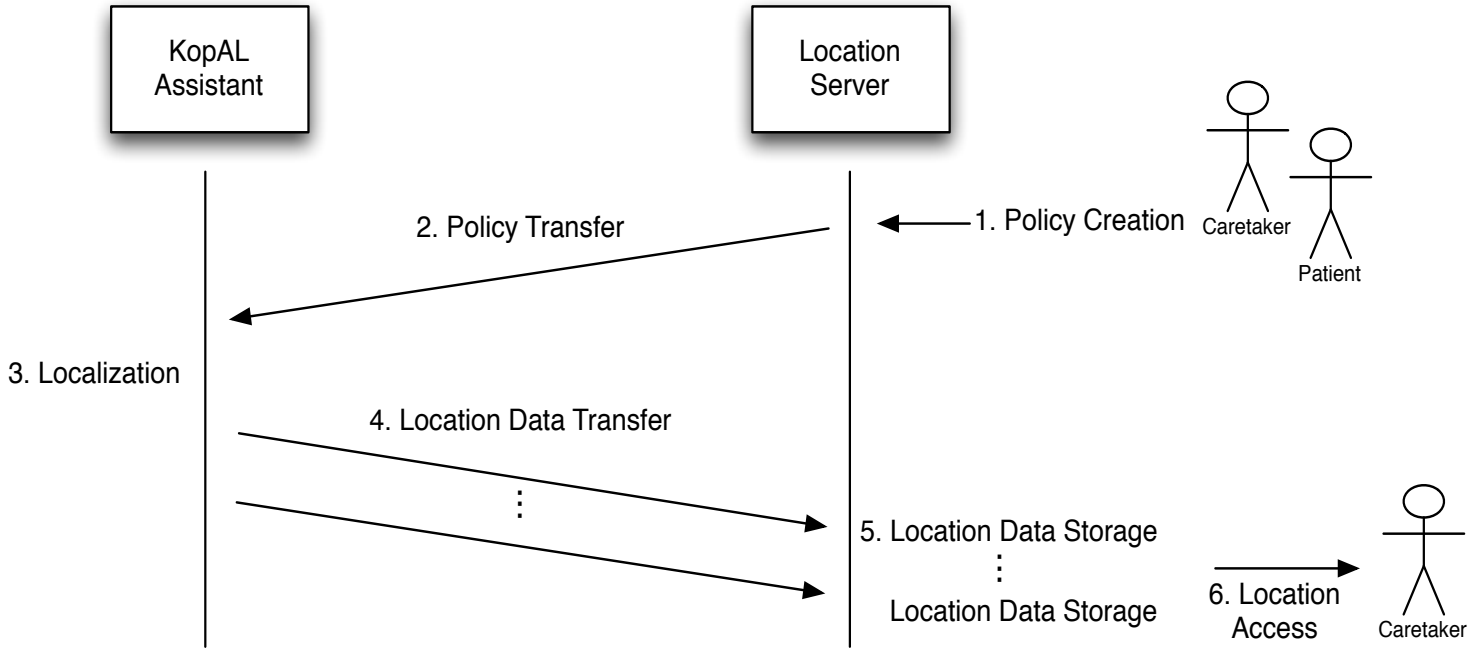
Data Privacy for Location Services

Question: How can the sensitive private location data of a patient be protected in the presence of different actors?

- Sensitive data stored as semi-structured XML-Documents
  - Location data
  - Access Policy
- (Distributed) Access Control Framework
  - Requests to resources must be evaluated at time of resource access
  - Deployment of trusted infrastructure
- Automated enforcement of authorisations

Data Privacy = Access Control + Usage Control

Workflow for Localization Assistance in KopAL



- Integrated management of access rights via Sticky-Policies
- The protected data are stored together with the usage policies as a Sticky Policy Object and can be referenced anytime by the system

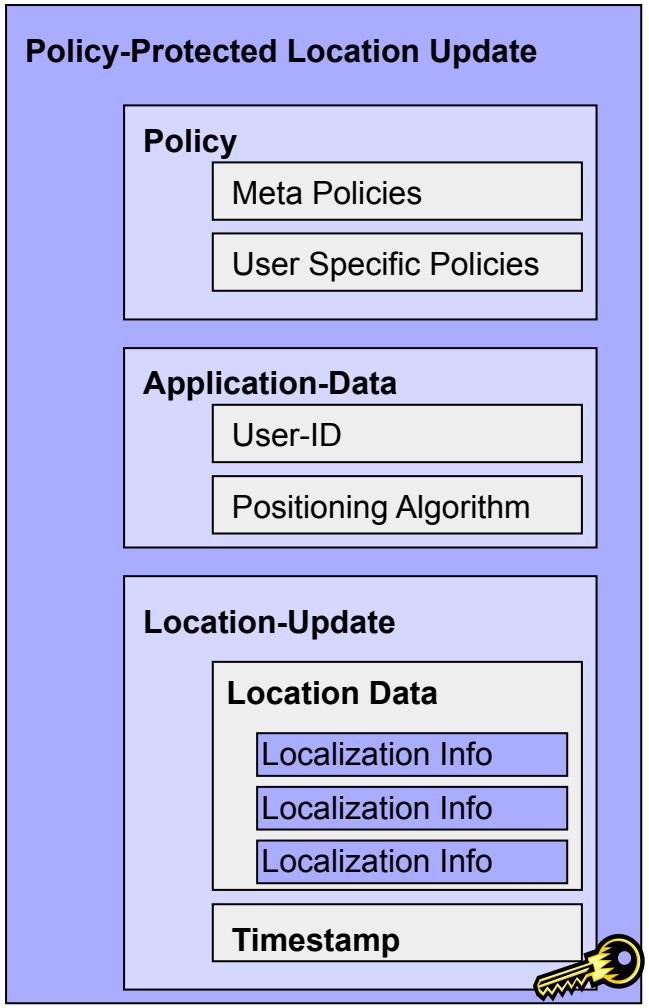
Data Privacy for Location Services

Use-case requires predefined Policy-Set:

- No access
  - Position updates are not send and stored
- Emergency only
  - Position updates are send
  - Caretaker can access location if ‘Emergency Button’ is pressed on the device
- Restricted access
  - Position updates are send
  - Caretaker can access location to find misplaced device (logging required?)
  - Caretaker is informed when person enters critical regions

Sticky Policies

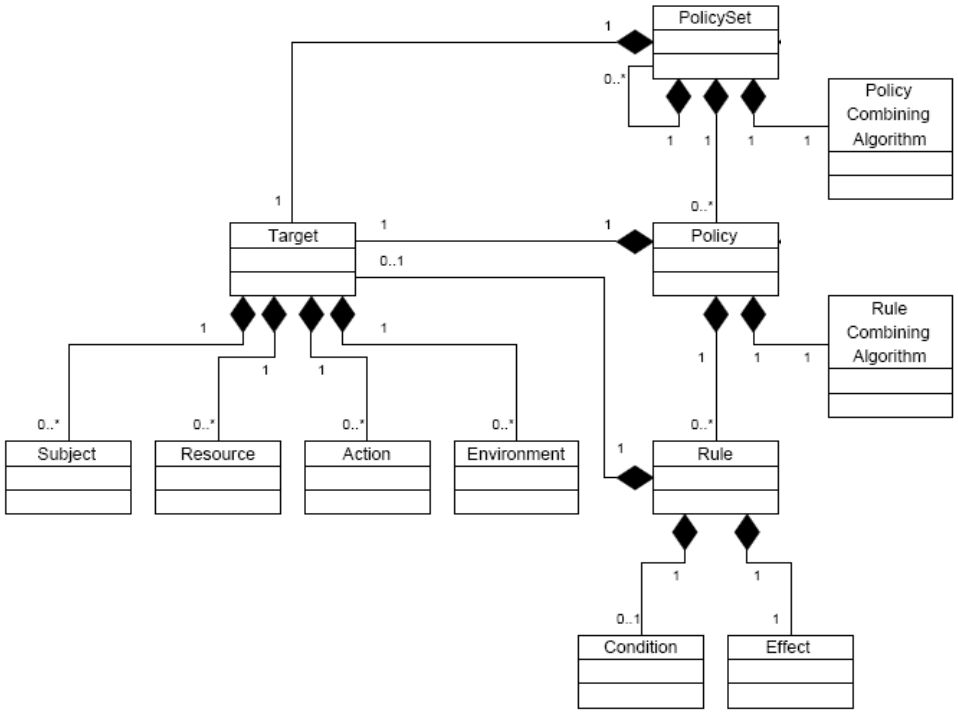
- The Policy-Store holds:
  - Meta Policies
  - User-generated Policies
- Application data about the patient includes:
  - User-ID
  - Positioning Algorithm
- The Location-Update contains information about:
  - Location Data
  - Timestamp



Policy Languages for Localization Data

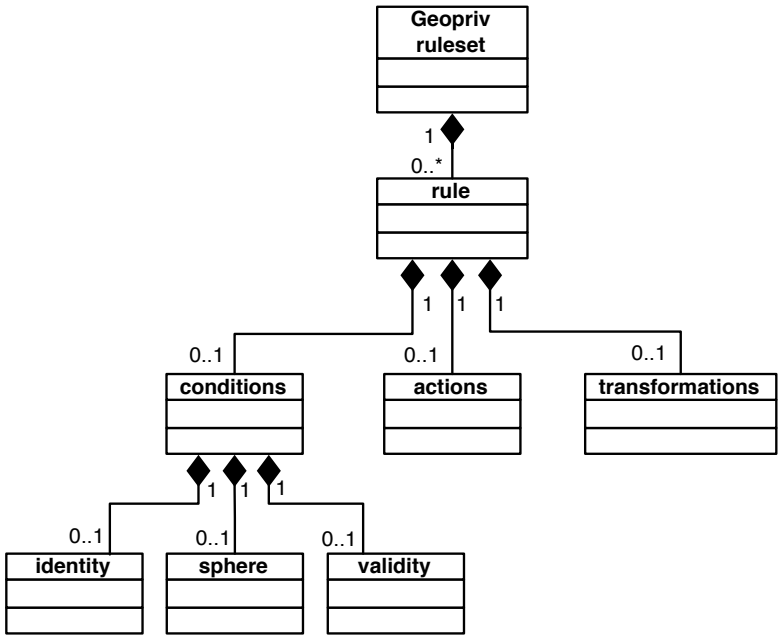
XACML

- eXtensible Access Control Markup Language (XACML) developed by OASIS, current version 2.0
- Generic Policy Language, as well as Request/Response Language



Geopriv – Common Policy

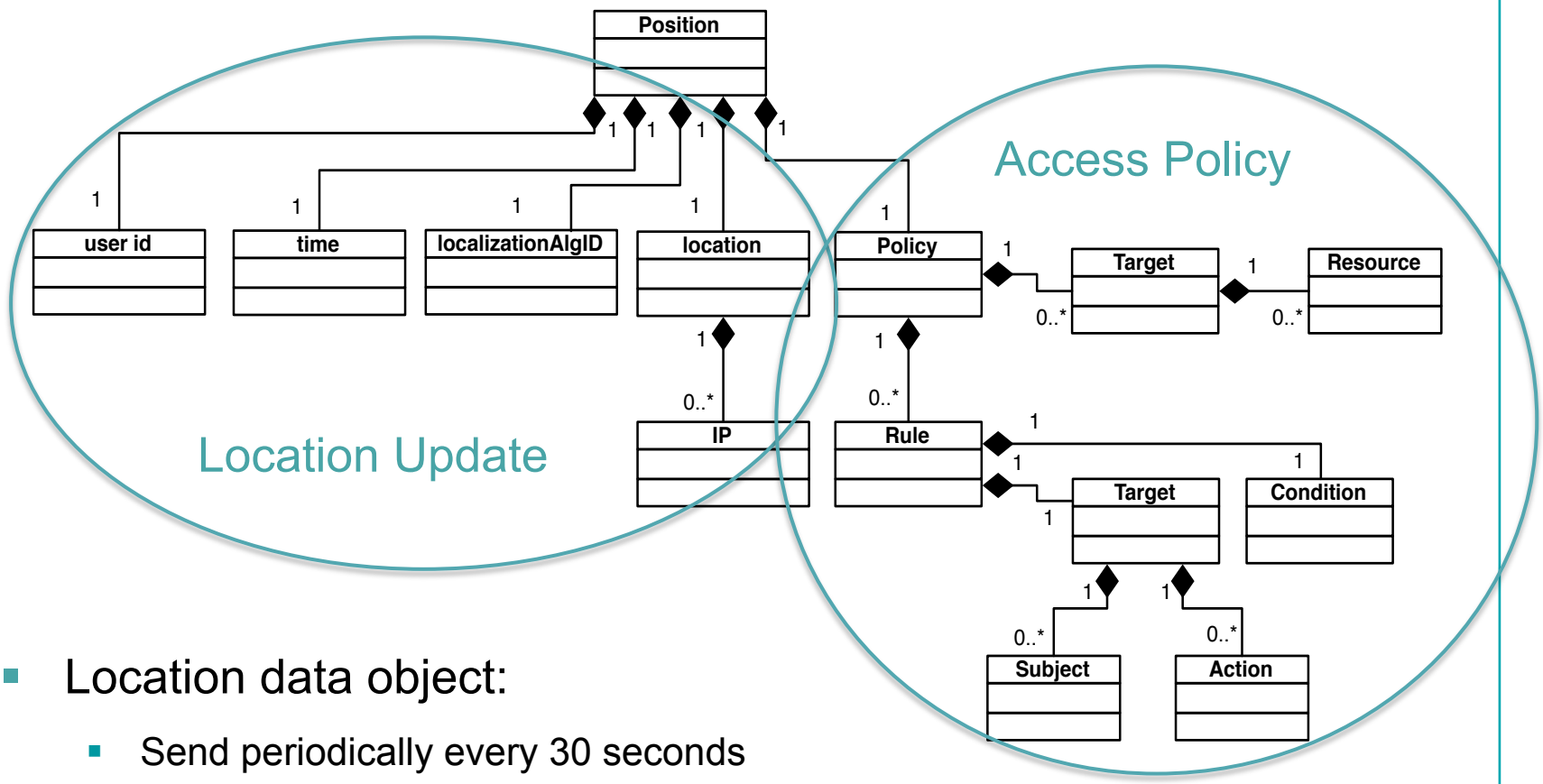
- Developed by the Geopriv WG of the IETF, RFC 4745
- Targeted Policy Language for expression of localization policies



Geopriv Common Policy

- (Some) characteristics of Geopriv:
  - Only positive authorisation rules allowed
  - Complete ruleset needs to be evaluated
  - No ability to explicitly specify purposes for data-use in policies
  - Targeted expressions for location transformation (obfuscate, reduce precision, …)
  - Policy combining is narrowly defined (generates the union over the matching permissions in the rule-set, returning the maximum value across the permission-set)
  - Currently no known implementations

XACML Datamodel



- Location data object:
  - Send periodically every 30 seconds
  - Server only stores a short history of values
  - Every location update contains complete policy
  - Location update is encrypted using RSA

Conclusion and Outlook

Conclusion

- Privacy friendly design
  - Coarse localization pattern
  - Short data retention periods
  - Policy protected data
- Minimal intrusion uppon the user
  - Set up once, continuous protection
  - Patiens can change their policy settings
- Extensions are under evaluation:
  - Invide other patients to signal presence
  - Use localization data to place reminders on wall terminals
  - ... (limited by patient needs)

A Privacy-Aware Localization Service

Thomas Scheffler
Beuth-Hochschule für Technik Berlin
University of Applied Sciences

Email: scheffler@beuth-hochschule.de
WWW: prof.beuth-hochschule.de/scheffler