Security for SWE Services

52north
exploring horizons

Overview

- Sensor Observation Service (SOS)
- Why do we need Security?
- Requirements
- Security Architecture
- Adaptation to the SOS interface
- Example
- Conclusion

Sensor Observation Service (SOS)

- Interface for accessing observations and sensor metadata
- Important Operations
  - GetCapabilities
  - DescribeSensor
  - GetFeatureOfInterest
  - GetObservation
  - RegisterSensor
  - InsertObservation

Why do we need Security?

- Non-public data → need for access control
- Example use cases:
  - SOS providing the positions of firemen during a forest fire
  - SOS containing information about the arsenic concentration within the drinking water → access for the public only after verification by experts
- GetCapabilities, DescribeSensor, GetFeatureOfInterest, GetObservation

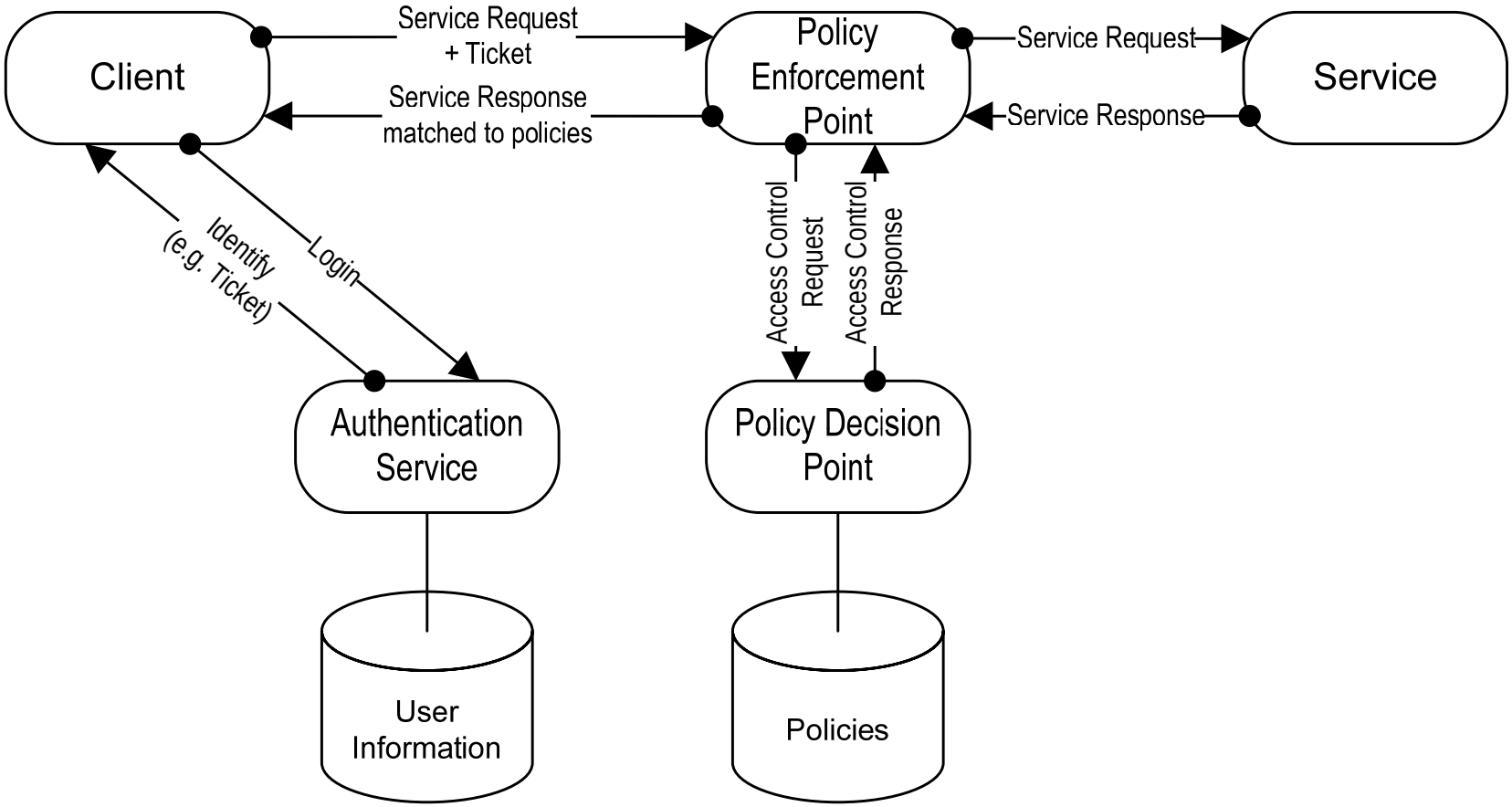
Why do we need Security?

- Transactional interface of the SOS allows inserting sensors and observations
- Not anybody shall be able to write into a SOS instance
- RegisterSensor, InsertObservation must be protected

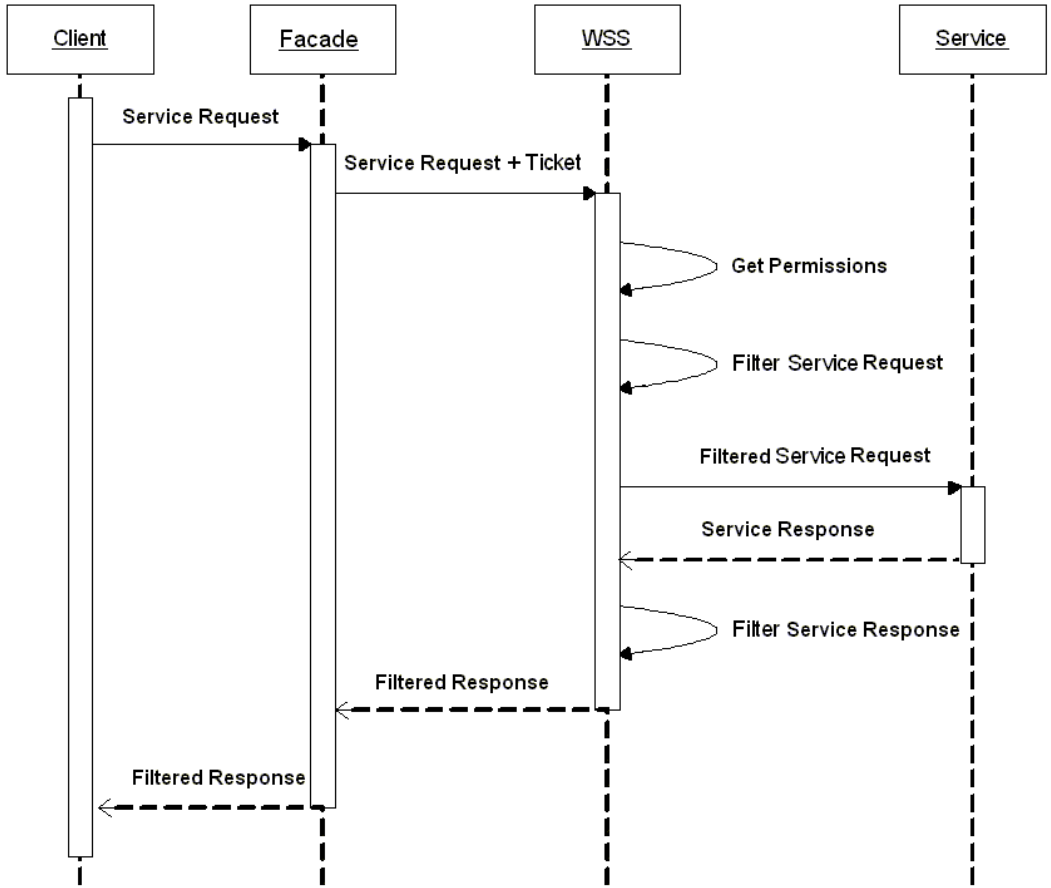
Requirements

- No changes to existing service interfaces → transparent integration
- Authentication
  - Single-sign-on
- Authorization → Control access by
  - Spatial criteria
  - Thematic criteria (observed properties)
  - Data quality

Security Architecture



Security Architecture

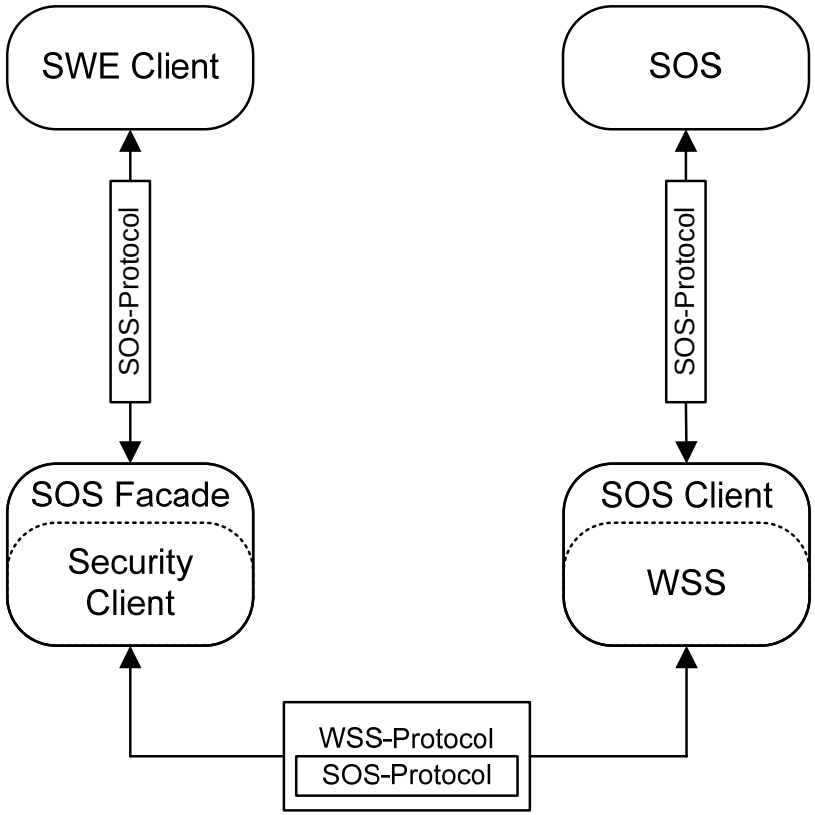


Adaptation to the SOS interface

- Based on 52° North security components
- Web Authentication Service (WAS)
  - Authentication of users
  - Issues a ticket based on the OASIS Security Assertion Markup Language (SAML)
- Web Security Service (WSS)
  - Policy Enforcement Point and Policy Decision Point
  - Filtering of requests and responses
- Web Security Client (WSC)
  - Web based interface for creating facades by entering user information (e.g. username and password)
  - Facades are visible to the client an act in the same way as the service secured by the WSS does

Adaptation to the SOS interface

- Nesting of protocols



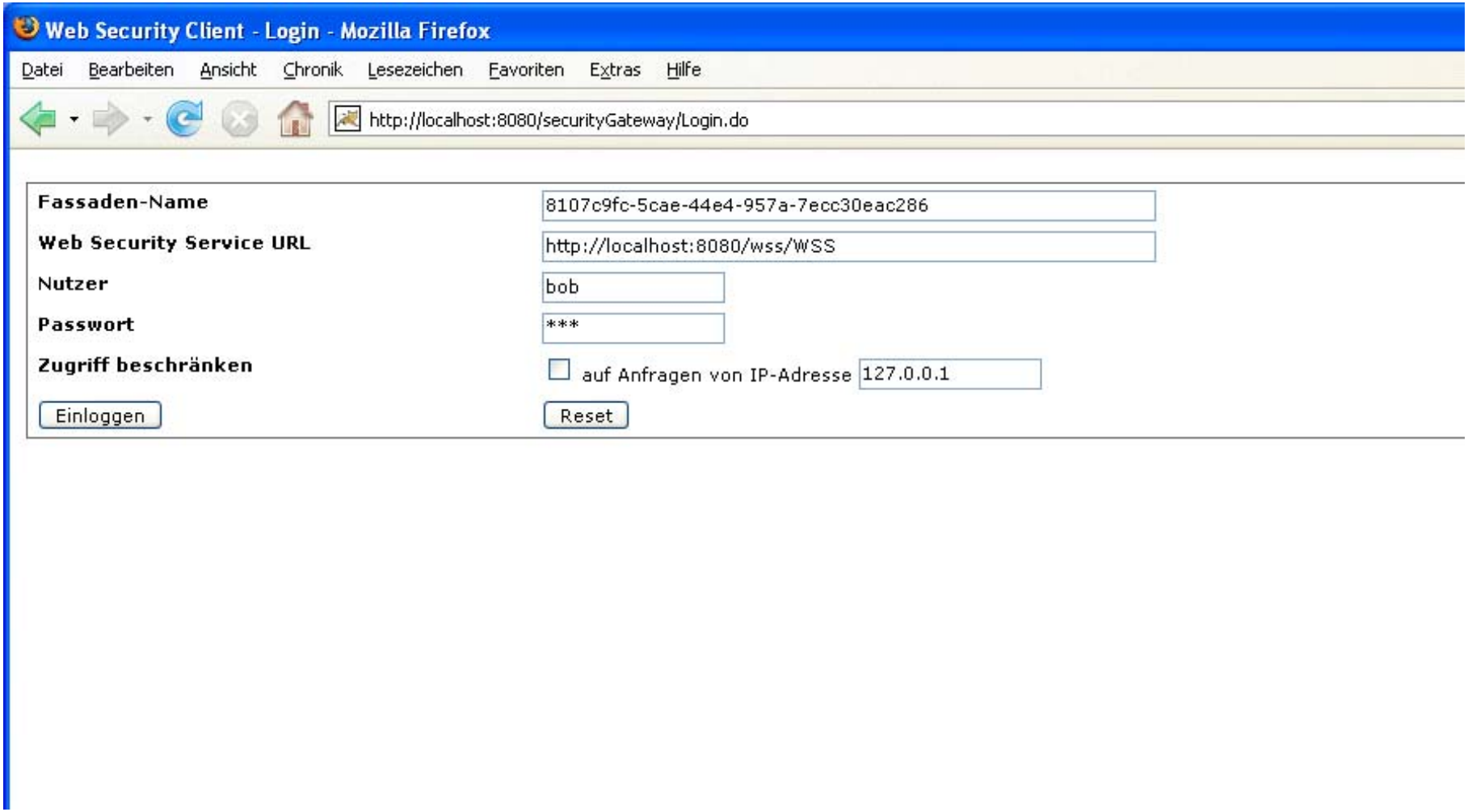
Adaptation to the SOS interface

- GetCapabilities
  - Request remains unchanged
  - Response must be filtered
    - Offerings
    - Sensors
    - Observed properties
    - Spatial and temporal extents
- DescribeSensor
  - Checks if the user is allowed to retrieve metadata for the requested sensor and prevents access if necessary
  - Response remains unchanged

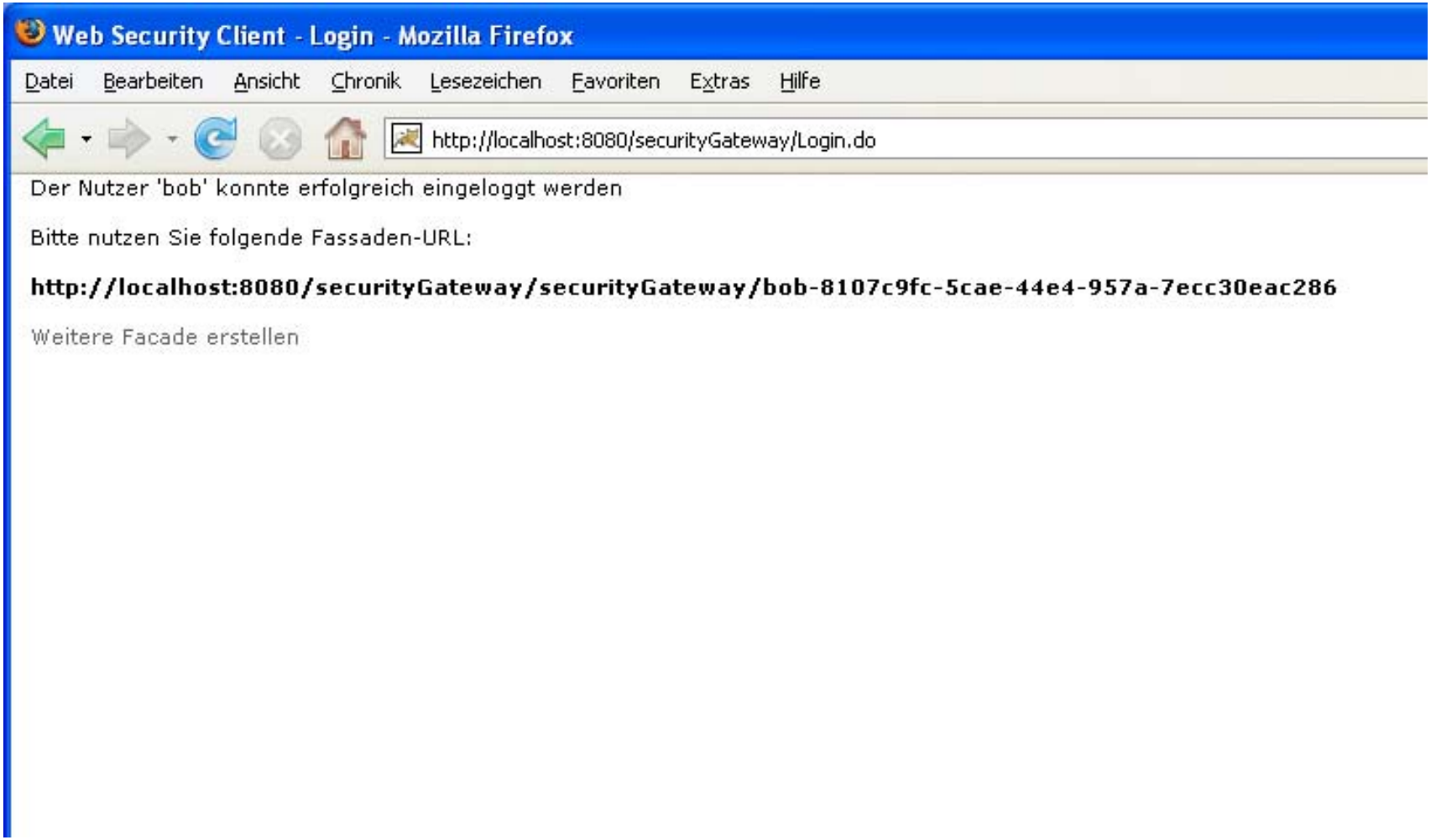
Adaptation to the SOS interface

- GetFeatureOfInterest
  - Checks if the user is allowed to query for the requested features and removes not allowed features
  - Response remains unchanged
- GetObservation
  - Filtering/modification of all requests so that only those resources are requested which are allowed to the user
  - Response remains unchanged
- Transactional Profile operations
  - RegisterSensor and InsertObservation
  - Control access on the Operation level

Example


Web Security Client - Login - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Favoriten Extras Hilfe
http://localhost:8080/securityGateway/Login.do
Fassaden-Name
8107c9fc-5cae-44e4-957a-7ecc30eac286
Web Security Service URL
http://localhost:8080/wss/WSS
Nutzer
bob
Passwort
***
Zugriff beschränken
auf Anfragen von IP-Adresse
127.0.0.1
Einloggen
Reset

Example


Web Security Client - Login - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Favoriten Extras Hilfe
http://localhost:8080/securityGateway/Login.do
Der Nutzer 'bob' konnte erfolgreich eingeloggt werden
Bitte nutzen Sie folgende Fassaden-URL:
http://localhost:8080/securityGateway/securityGateway/bob-8107c9fc-5cae-44e4-957a-7ecc30eac286
Weitere Facade erstellen

Example

- GetCapabilities
  - Bob is allowed to see everything (see bob_caps.xml)
  - Alice is only allowed to see the temperature for a feature (see alice_caps.xml)

Conclusion

- Good example how a SOS can be secured
- The implementation will be made available through 52° North (www.52north.org)
- Testing in real world scenarios within the OSIRIS project (www.osiris-fp6.eu)