



Concept of GDI-DE & Security Practices

2nd IOC Services Team Meeting
18.01.2010

Jan Grohmann, Jan.Grohmann@bkg.bund.de
Christian Elfers, c.elfers@conterra.de

Outline

- Security Concept of GDI-DE (Jan)
- Security Practices for short term security solutions (Christian)
 - Considerations & Concepts
 - Solution Demonstration (securityManager based on 52°north security modules)

Requirements

How it began:

- tender in the context of the follow-up of the architecture document of sdi germany

What we need:

- concept for access control
- support of single sign on
- consider the decentralized infrastructure (use the decentralized identity provider)
- consider standards like ISO, ITU, OGC, OASIS, W3C, ..

Proposal

Short-term period:

- use HTTP Authentication (Basic and Digest) with HTTPS to secure services

Mid-term period:

- exchange authentication information with SAML 2.0
- declare and enforce access rights with XACML 2.0 and GeoXACML 1.0
- use HTTPS for communication with web browser based clients to ensure confidentiality and integrity (SAML SSO Browser Post Profile)
- use WS-Security for communication with desktop based clients to ensure confidentiality and integrity (SAML Enhanced Client Profile)
- possible realisation with Shibboleth

Actual tasks and further steps

Actual tasks:

- review the concept within the working group (also from the Federal Office of information security (BSI))
- develop a prototype as proof of concept to gain experiences

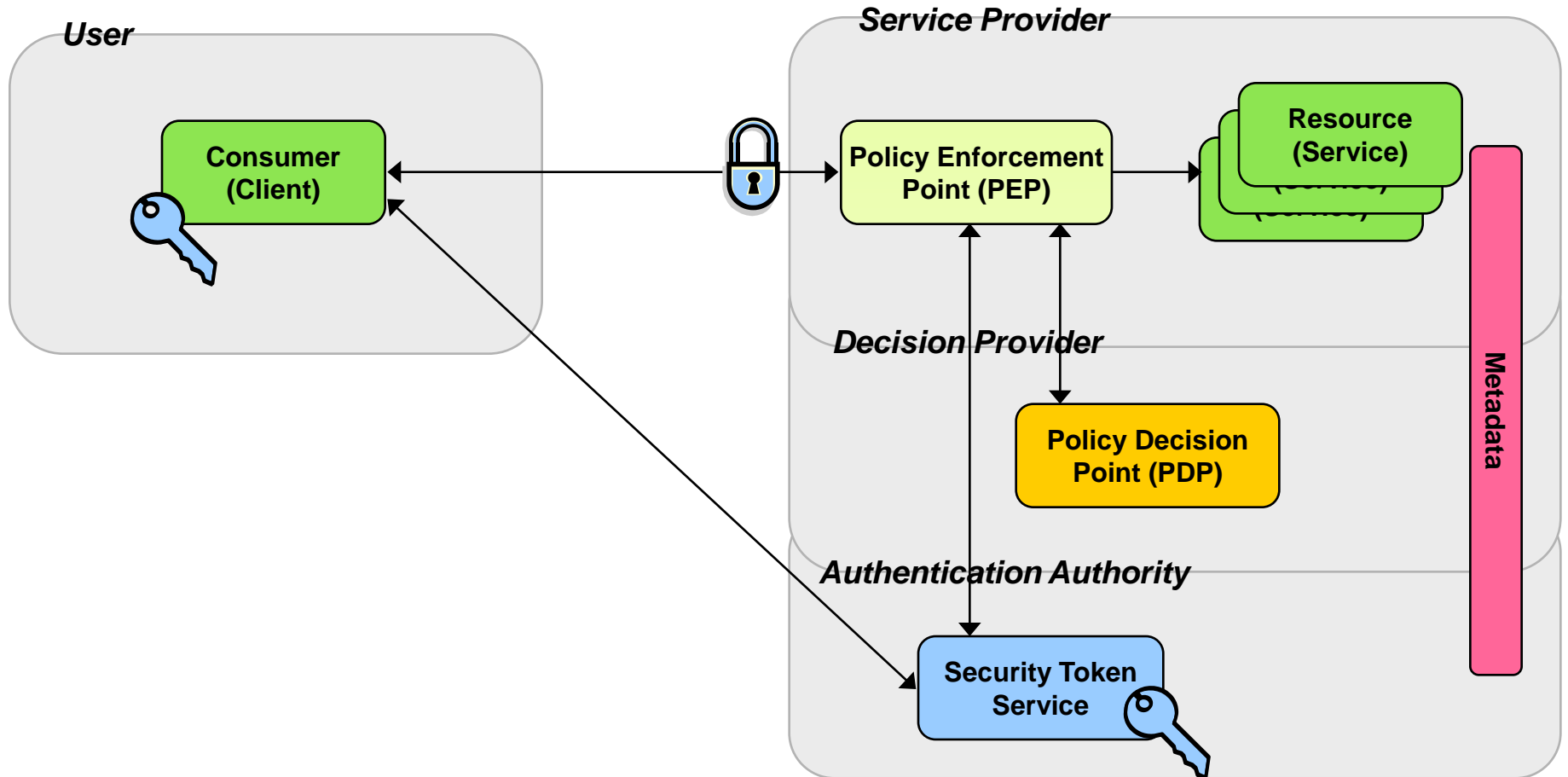
Further steps (will be a challenge):

- agreement on the attributes and roles which will be necessary for authentication
- agreement on the meaning and the declaration of access rights
- service chaining (long-term)
- e-commerce and licensing (long-term)
- ...

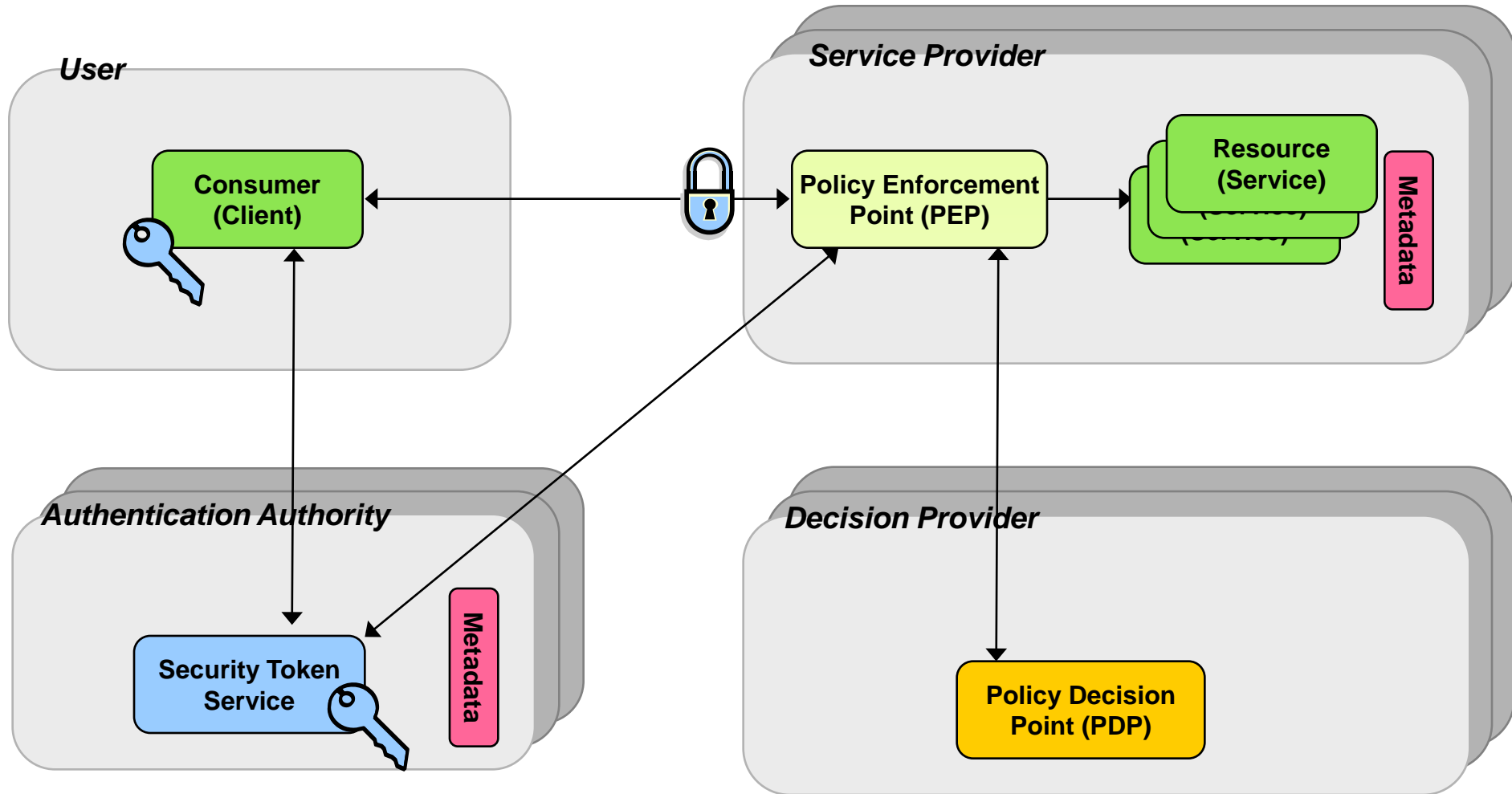
Practices - Considerations

- Security for SDI
 - Organizational/business model & tasks/responsibilities
 - Technology & impact on existing standards
 - Separation in 3 types of involved parties: users, data-/service providers, facilitators
- Main tasks for security in SDIs: Authentication & Authorization
- Organizational model & the business model question
 - Centralized and/or decentralized authentication authorities?
 - Multiple authentication authorities? Is there a lead?
 - Sharing of users information, privacy requirements (hiding/sharing, account linking, etc)
 - Who manages access policies? Who applies/enforces them?
 - Who is responsible to accomplish which tasks? What are member state internal tasks, what is facilitated on the european level? What is the role of the geoportal in that context?
- Important to answer these the before defining the technical approach (technology needs to support the model but might be implemented stepwise);
- Additional technical aspects:
 - Leverage existing standards and concepts from IT industry, there is only little geo-specific
 - Technology should have no impact on standard service interfaces (or be supported)
 - Use standards where absolutely needed (external/internal aspects)

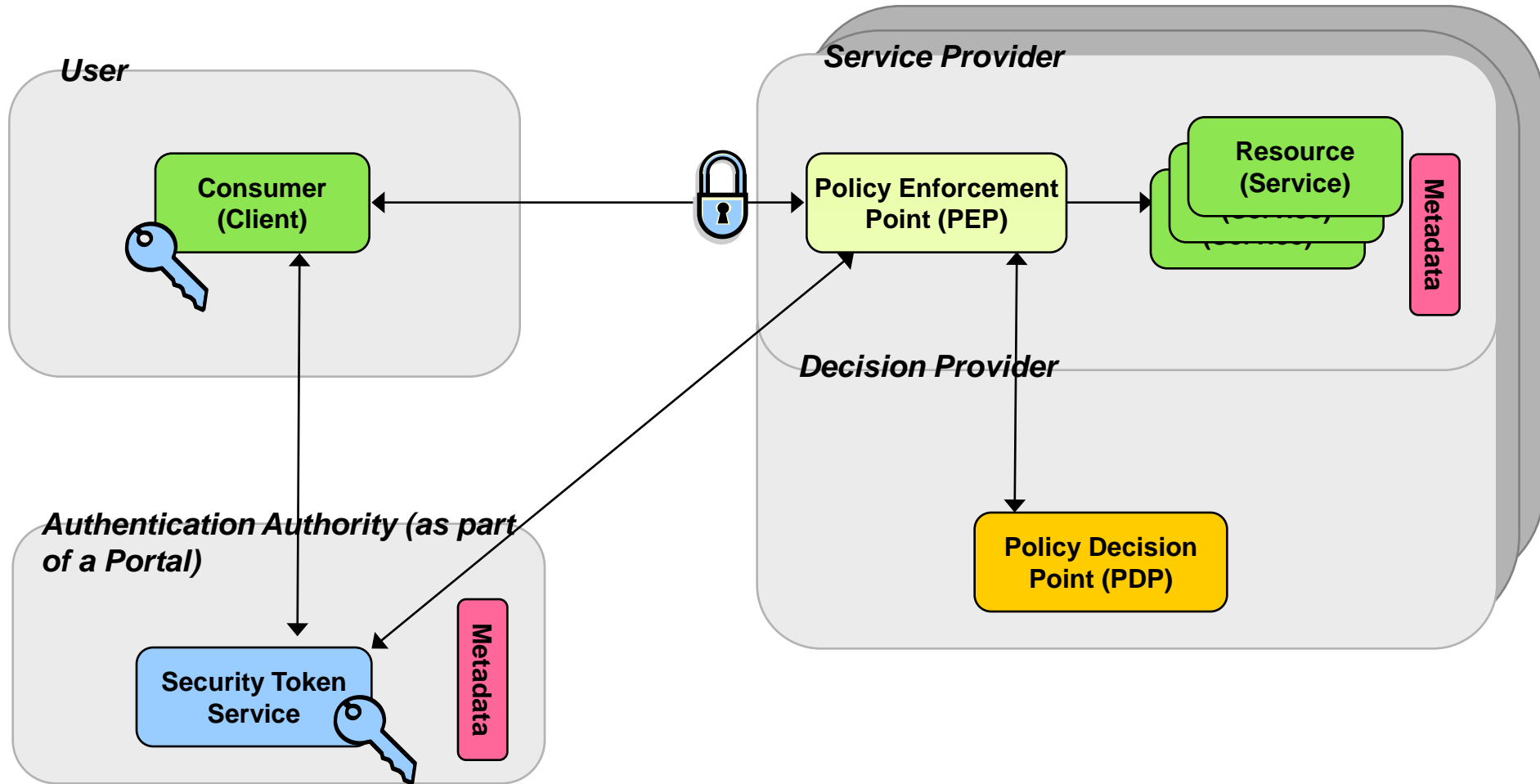
Concept's – All-in-one setup



Concept's – Complete Distribution

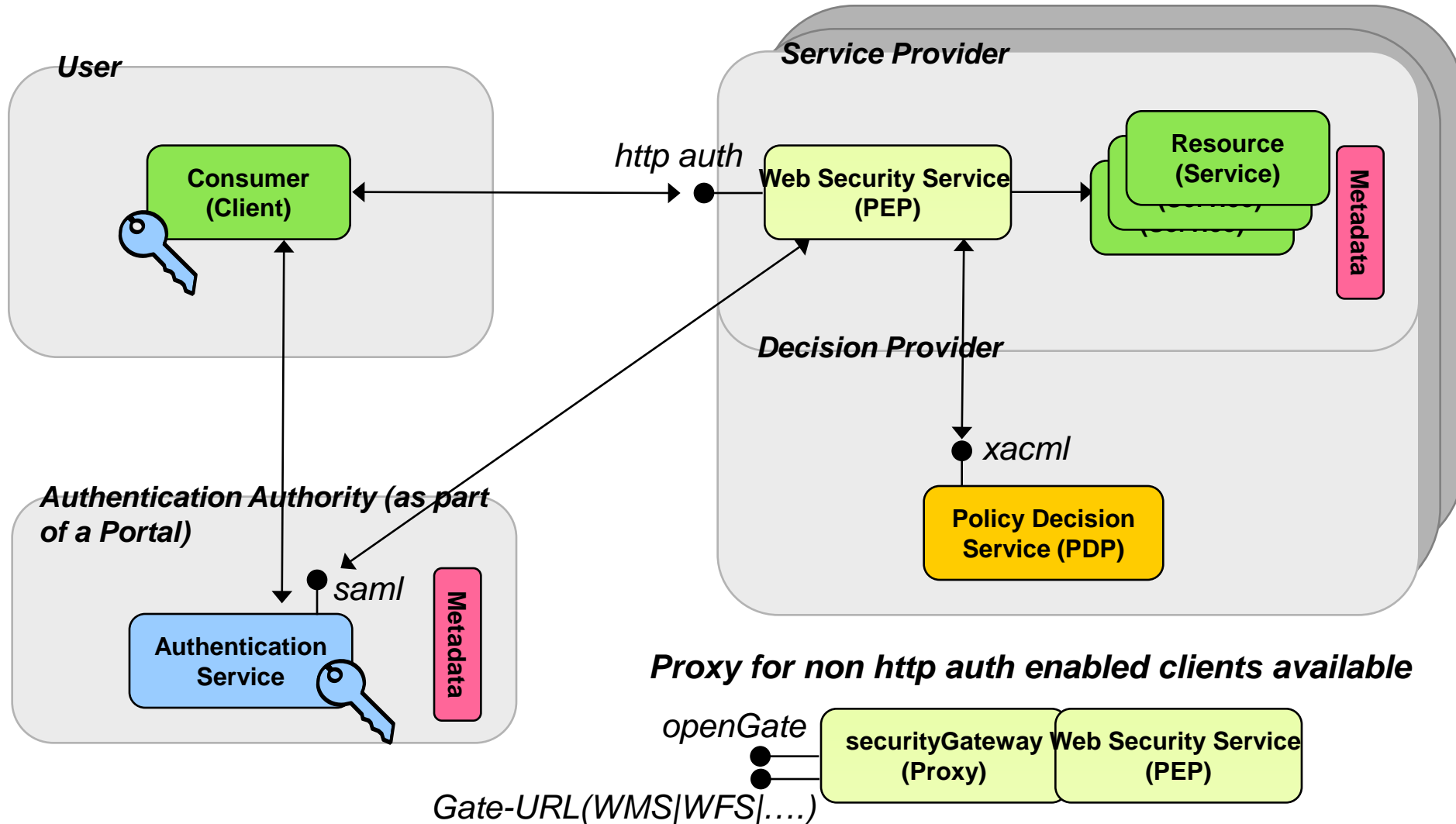


Concept's – A Typical Example



A Typical Example

- implementation with 52°north/ securityManager



Demo

Considerations on how to move ahead

- Define the model first
 - Think of roles, responsibilities, dependencies
 - Requirements on different levels: individual organisation, (sub) member state, european
 - Identify relevant activities/policies (again on different levels)
 - It is unlikely that all member states will follow the same approach; so what is the smallest common denominator?
 - Connect it to the architecture(s) (MS & Europe)
- Implementation
 - A step-wise approach is good as it reduces complexity
 - Appropriate standards (SAML, Liberty, W3C, OASIS, WS-Security, ...) &
- Technologies
 - HTTP Auth has minimal impact
 - Lots of other technology approaches out there
- GeoRM is more than Security/Access Control
 - Additional roles & tasks: license creation/offering/conclusion, license enforcement
 - Additional technical aspects: transport and encoding of licenses, service interfaces