

Enterprise and e-business Security Solutions



Using SPML to provision dynamic XACML rules to manage privacy and access control in Web Security

Michel Hétu

Anton Stiglic Msc.

Claude Vigeant Eng.

Solutions for a changing world

Global Trust I&AM Capabilities

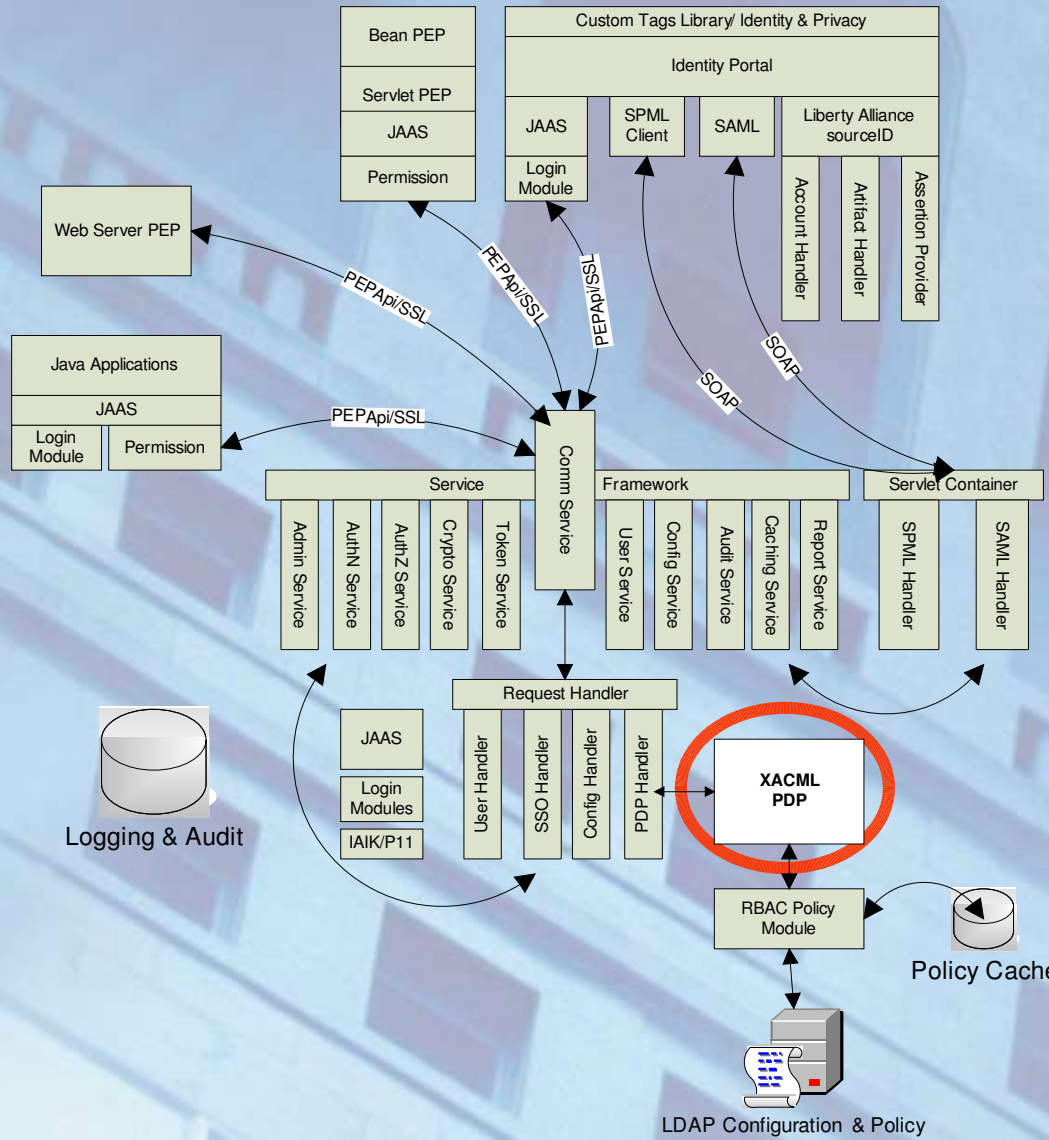
- **Identity Management**
 - Login/Logout
 - Registration/De-Registration
 - Self-Care
 - Password Recovery
- **Privacy**
 - Opt-in/Opt-out
 - Consent
 - Report of user info disclosures
 - Amendment
- **Access Control**
 - Single Sign-On
 - Authentication
 - Authorization
 - Audit & Logging
- **Provisioning**
 - Users
 - Roles
 - Policies
- **Identity Federation**
 - Liberty Alliance
 - SAML
- **LDAP Directory support**



Global Trust Key Features

- **Delegated Administration**
- **Role-Based Access Control**
- **Identity Portal**
- **Single Sign-On (SSO)**
- **JAAS Authentication Framework**
- **XACML Policies & Conditions**
- **SAML and Liberty Identity Administration**
- **Centralized Audit & Logging**
- **Centralized Policy Administration**
- **Distributed Policy Enforcement & Evaluation**
- **Auto-Registration of PEPs**
- **SPML Provisioning**
- **Resource Explorer**

Where XACML stands in Global Trust



PIPEDA Principles

- **Consent**
- **Limiting use, Disclosure & Retention**
- **Accuracy Verification**
- **Safeguards**
- **Openness**
- **Individual Access**
- **Challenging Compliance**
- **Accountability**

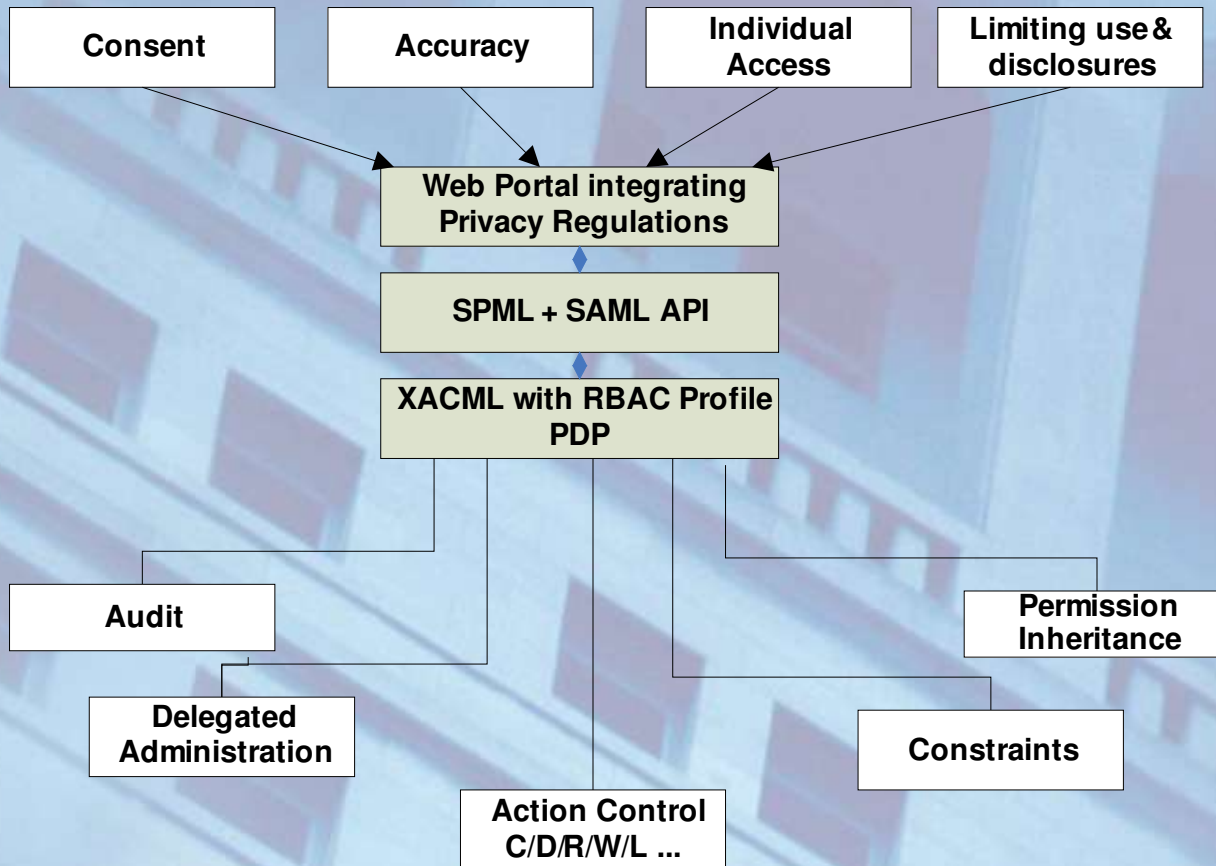
PIPEDA Enforcement

Principles	Enforcement
Consent	Via the web portal using an SPML Client API to assign or de-assign roles
Limiting use, Disclosure & Retention	Via the web portal using SPML Client API to create new policies and rules
Accuracy Verification	Via the web portal using a Verification form
Safeguards	I&AM, firewall, VPN, SSL Encryption, etc

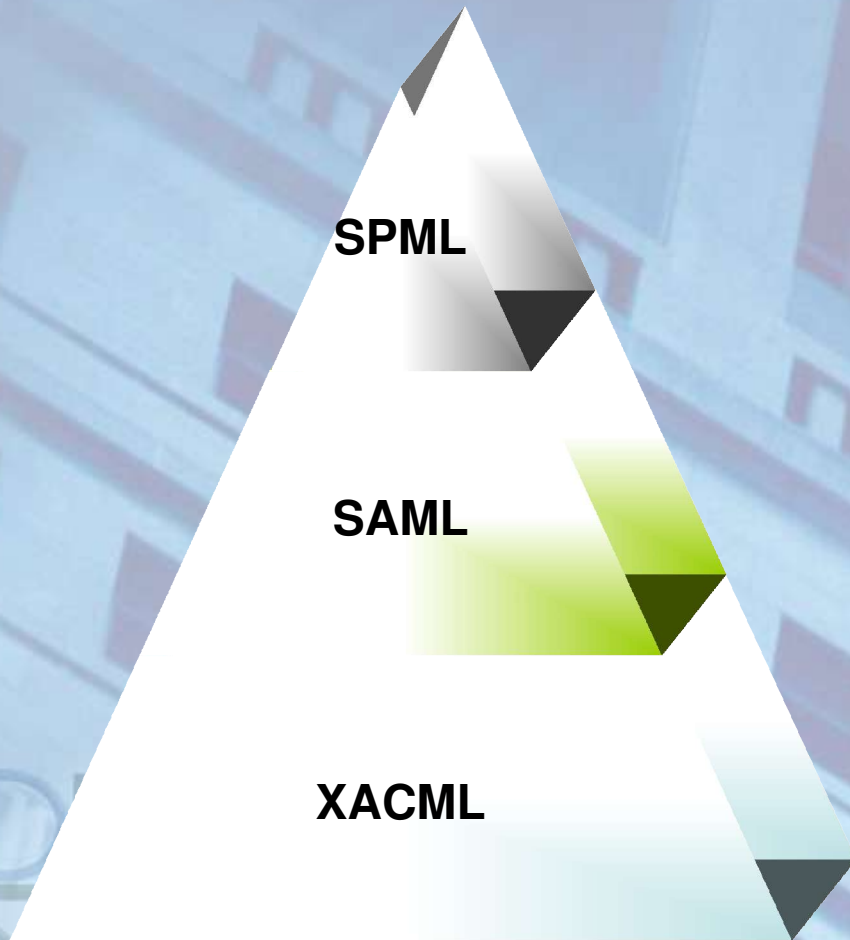
PIPEDA Enforcement (cont.)

Principles	Enforcement
Openness	Publish Privacy Policies on web site
Individual Access	Via the web portal using custom tags API or else to display digitally signed audit log of all activities
Challenging Compliance	Complaint procedures via web portal forms
Accountability	An individual must be appointed in the enterprise to verify the PIPEDA compliance. This individual has an administrative role in the I&AM allowing him to do so

The Picture



A Pyramid and an OASIS



- **Web Portals Provision Users & Rules**
- **PEP Authenticates & Authorizes via SOAP**
- **RBAC Policy Decision Point**

SPML at a glance

Service Provisioning Markup Language is made of three components:

- **RA (The web client.)**

A Requesting Authority is a software component that issues well formed SPML requests to a known SPML service point.

- **PSP (The I&AM server)**

A Provisioning Service Point is a software component that listens for, processes and returns the results for well formed SPML Requests.

- **PST (An LDAP Directory)**

A Provisioning Service Target is a software component that is seen as the end point or a given provisioning action.

SPML Operations

The following operations are available:

- **AddRequest**
- **CancelRequest**
- **DeleteRequest**
- **ModifyRequest**
- **SearchRequest**
- **etc.**

The objectclass attribute

The objectclass attribute specifies the class of the object being created such as:

- User
- Role
- Policy
- Rule
- Resource

```
private void addPolicy(String name, String rule)
{
    attributes = new HashMap();
    AddRequest request = new AddRequest();
    request.setObjectClass("policy");
    attributes.put("name", name);
    attributes.put("rules", rule);
    attributes.put("enabled", "true");
    request.setAttributes(attributes);
    SpmlResponse response = doRequest(request);
}
```

SPML Client API

- **Used to provision objects including XACML rules and policies**
 - addUser(String, String)
 - deleteUser(String, String)
 - addBusinessRole(String, String)
 - deleteBusinessRole(String, String)
 - assignBusinessRoleToUser(String, String)
 - unAssignBusinessRoleToUser(String, String)
 - addBusinessResource(String, String)
 - deleteBusinessResource(String, String)
 - addBusinessRule(String)
 - deleteBusinessRule(String)
 - assignBusinessResource(String, String)
 - unAssignBusinessResource(String, String)
 - addBusinessPolicy(String, String)
 - deleteBusinessPolicy(String, String)
 - etc.

Let's put it together

- **When a user consents to disclose personal information, the SPML API is used to assign the user, group or department to the role using the method:**
 - `assignBusinessRoleToUser(String, String)`
- **When a user wants to limit use of personal information (opt-in, opt-out), XACML policies & rules are created using the methods:**
 - `addBusinessPolicy(String, String, ...)`
 - `addBusinessRule(String, ...)`

Let's put it together (cont.)

- **When the user wants to verify who accessed his personal info, a custom tag sends a request to the I&AM server to return all activities from the audit log regarding a user based on search filters.**

2005-04-08 10:18:10, facility specialist, Harvey BedRoom, read, myPHI,...

2005-04-08 10:18:10, nurse, Clare Doolittle, read, myPHI, ...

2005-04-08 11:12:19, doctor, Roger Frankenstein, update, myPHI, ...

2005-04-09 10:18:10, HMO insurer, Joe Money, read, myPHI, ...



Why we chose XACML

- **Flexible authorization model**
- **RBAC Support**
- **Allow Policy Distribution (import/export) based on XML documents**
- **Obligations returned on PDP evaluation support authentication assurance level**
- **Good open source implementation available from Sun**
- **Sun implementation resolves the standard Buy/Develop issue**
- **Extensible system (Policy Finder, Attribute Finder, Resource Finder)**
- **Used in conjunction with a policy cache, the PDP can evaluate close to a thousand of requests/sec on a small server (2.4Gz & 512 Mb)**
- **Natural fit with other standards like SAML or SPML**
- **OASIS Standard**
- **Market acceptance**

XACML in the Privacy world

Allows Access Control Policy to be expressed in XML. For HealthCare, XML rules could be like:

- 1. A person may read any record for which he or she is the designated patient.**
- 2. A person may read any record for which he or she is the designated parent or guardian, and for which the patient is under 16 years of age.**
- 3. A physician may write any medical element for which he or she is the designated primary care physician, provided an email is sent to the patient,**
- 4. An administrator shall not be permitted to read or write medical elements of a patient record.**

XACML Profile for RBAC

XACML Profile for Role Based Access Control allows to deal with meaningful job function within the context of an organization

- Patient**
- Admission Clerk**
- Ward Scheduler**
- Facility Specialist**
- Registered Nurse**

RBAC Security Model

User	Role
John	Admission Clerk
Jane	Ward Scheduler
Amanda	Registered Nurse
Anna	Facility Specialist

Permission	Role
Admission Proc	Admission Clerk
Discharge Proc	Admission Clerk
Transfer Proc	Ward Scheduler Facility Specialist
Lab Order Proc	Registered Nurse

Role	Domain
Admission Clerk	Patient Management
Ward Scheduler	Facility Management
Registered Nurse	Care Provider
Facility Specialist	Facility Management

Permission	Resource
Admission Proc	HL7 A01
Discharge Proc	HL7 A03
Transfer Proc	HL7 A02
Lab Order Proc	HL7 ORC



Navigation

- Global Trust
 - ou=People,dc=okiok,dc=com
 - Roles
 - Business
 - ou=People,dc=okiok,dc=com
 - QA
 - TransGlobal Consultir
 - HealthCare
 - Facility Manageme
 - Care Provider
 - Patient Manageme
 - Gouvernement du Q
 - Role1
 - Administration
 - GTAdministrator
 - RoleAdministrator
 - DomainAdministra
 - SeniorAdminist
 - Policies
 - Authentication
 - Authorization
 - Business
 - Policies
 - Rules
 - Actions
 - Administration
 - Conditions
 - Resources
 - Configuration

POLICIES

Authentication Authorization

List Policies Methods Policies Rules Conditions Actions Virtual resources

To assign resources, actions, and conditions to an authentication policy rule:
 - To select the rule, use the Policy rule name drop-down list box below. You will see three lists of resources, actions, and conditions currently assigned to the rule.
 - To add additional resources, actions, and conditions to a list, select them from the Policy Components tree on the right.
 - To remove one or more rules from a list, select them, then click the appropriate Remove button.
 - To apply the three lists to the selected rule, click Update.

Business Administration

Policy rule description

* Policy rule name: Admission_Proc

Description: Admission Procedure Rule

Resources and actions

* Resources: /Schema[@name='HL7']/ElementType[@content='eltOnly' and @model='closed' and @name='A01']

Remove

* Actions: update

Remove

Conditions

Conditions

Remove

Rule effect

Effect: Permit Deny

Policy rule state

Rule enabled:

Save Cancel

Rule components - Business

Policy Components

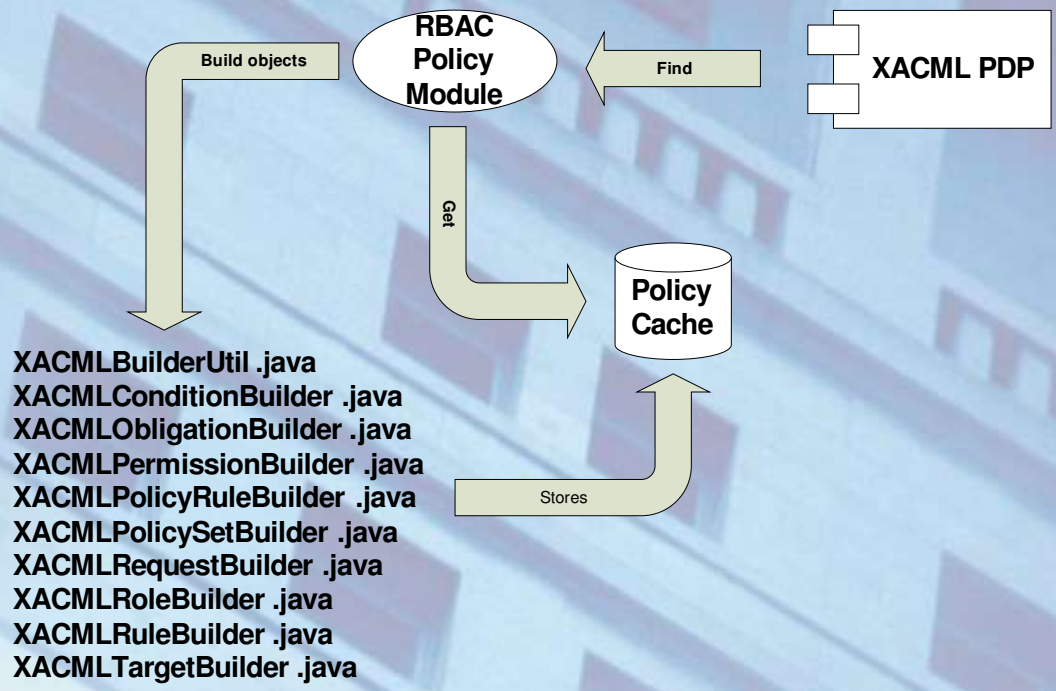
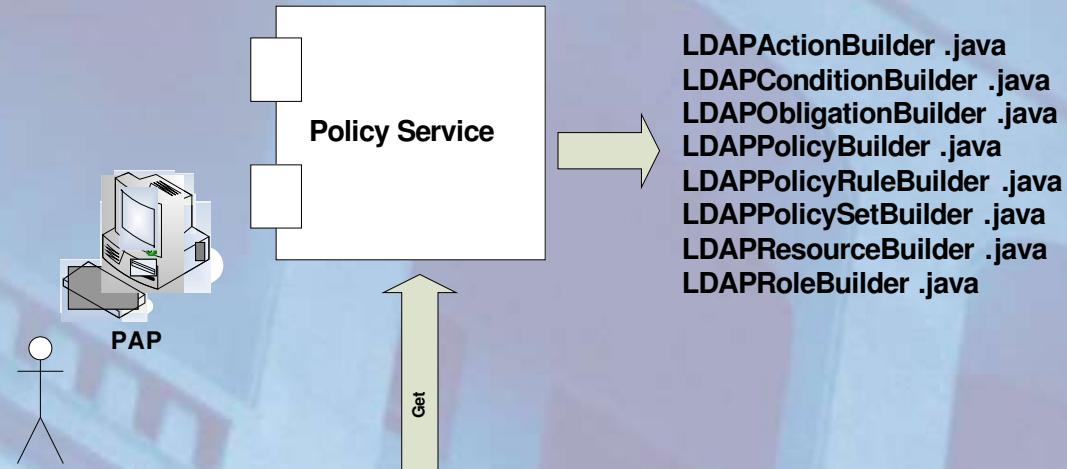
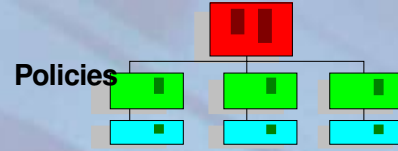
- Resources
 - www.okiok.com
 - J2EE Filter
 - GlobalTrust Proxy
 - Global Trust PEP
 - Virtual resources
 - Files
 - <Schema name="HL7" >
 - <ElementType content="eltOnly" model="closed" name="PID" >
 - <ElementType content="eltOnly" model="closed" name="A01" >
 - <ElementType content="eltOnly" model="closed" name="A02" >
 - <ElementType content="eltOnly" model="closed" name="A03" >
 - <ElementType content="eltOnly" model="closed" name="A04" >
 - <ElementType content="eltOnly" model="closed" name="A05" >
 - <ElementType content="eltOnly" model="closed" name="A06" >
 - <ElementType content="eltOnly" model="closed" name="A07" >
 - <ElementType content="eltOnly" model="closed" name="A08" >
 - <ElementType content="eltOnly" model="closed" name="A09" >
 - <ElementType content="eltOnly" model="closed" name="A10" >
 - <ElementType content="eltOnly" model="closed" name="A11" >
 - <ElementType content="eltOnly" model="closed" name="A12" >
 - <ElementType content="eltOnly" model="closed" name="PR1" >
 - <ElementType content="eltOnly" model="closed" name="IN1" >
- Actions
 - create
 - delete
 - read
 - update
 - write
 - Conditions

Reload tree

Tailoring Sun's XACML Policy Finder

The main Global Trust extension to the Sun's XACML PDP is about the Policy Finder. The module characteristics are:

- **The module implements the XACML Profile for RBAC**
- **The module load policies in cache using the Policy Service when the PDP calls init()**
- **The policies are translated from their PCIM LDAP representation to their XACML form by builders**
- **The findPolicy method searches the cache for policy matches for the maximum performance**
- **The module implements Observer to detect Policy changes & reload cache online**



Audit Trail

Privacy calls for a strong accountability. Digitally signed audit messages help to enforce this requirements.

- **Audit Message contains:**
 - **Timestamp**
 - **Audit Event**
 - Authentication
 - Authorization
 - User Management
 - Policy Management
 - **Subject (Authentication Ticket + UID)**
 - **Digital Signature**
 - **Resource**

Questions ?

Thank you!