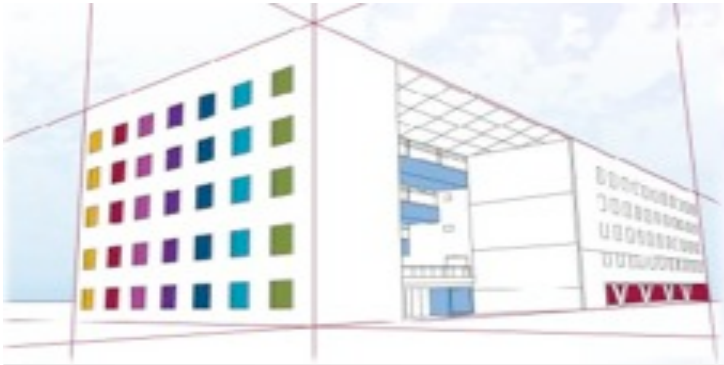


CNRS - INPT - UPS - UT1 - UTM

Institut de Recherche en Informatique de Toulouse

Une Vision Pour un Contrôle d'Accès Adaptatif aux Systèmes de Santé Pervasifs

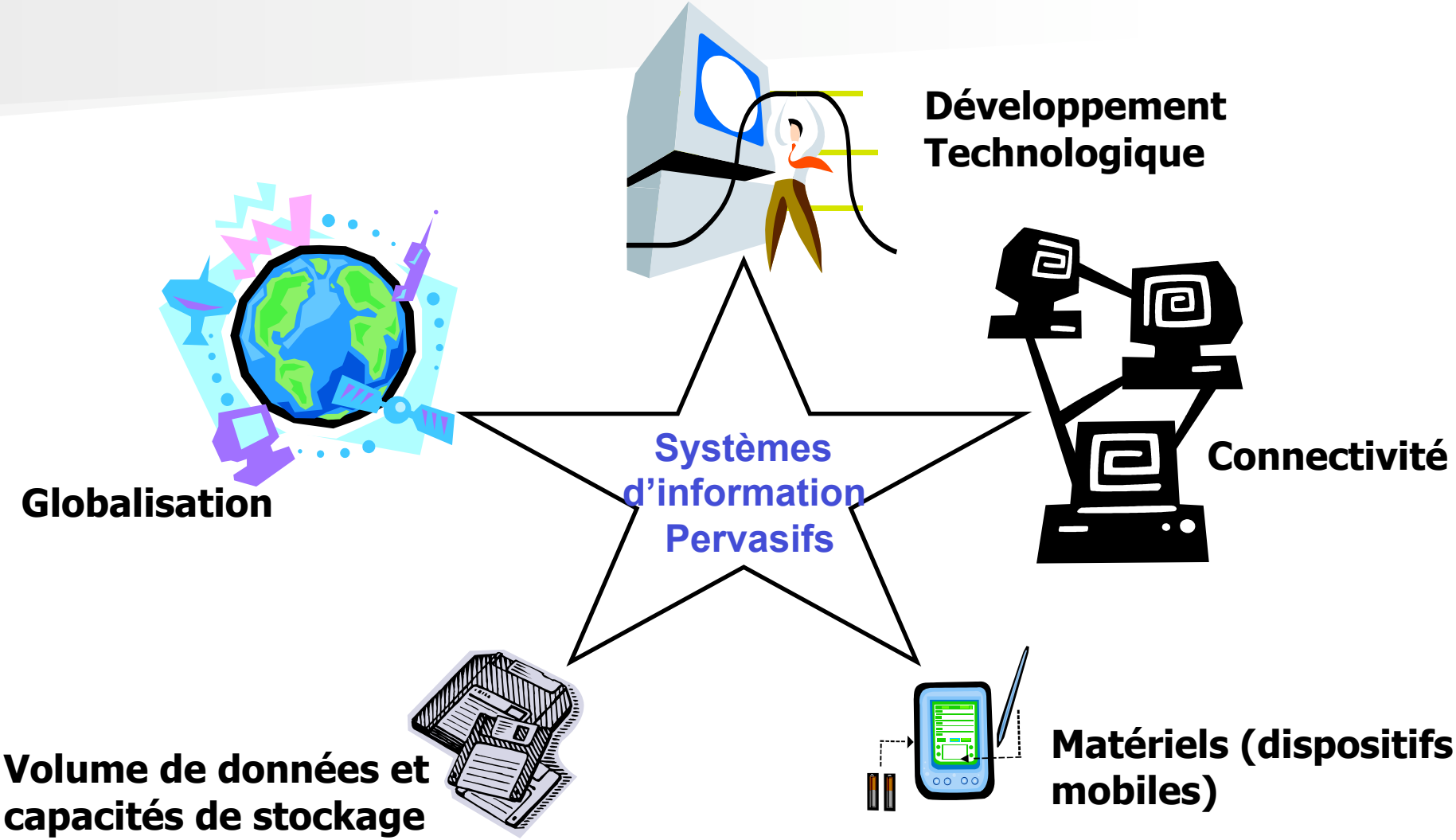
Présenté par: **Dana Al Kukhun**

Directrice de Recherche: **Pr. Florence Sèdes**

IRIT – SIG, Université Paul Sabatier

{Kukhun, sedes}@irit.fr

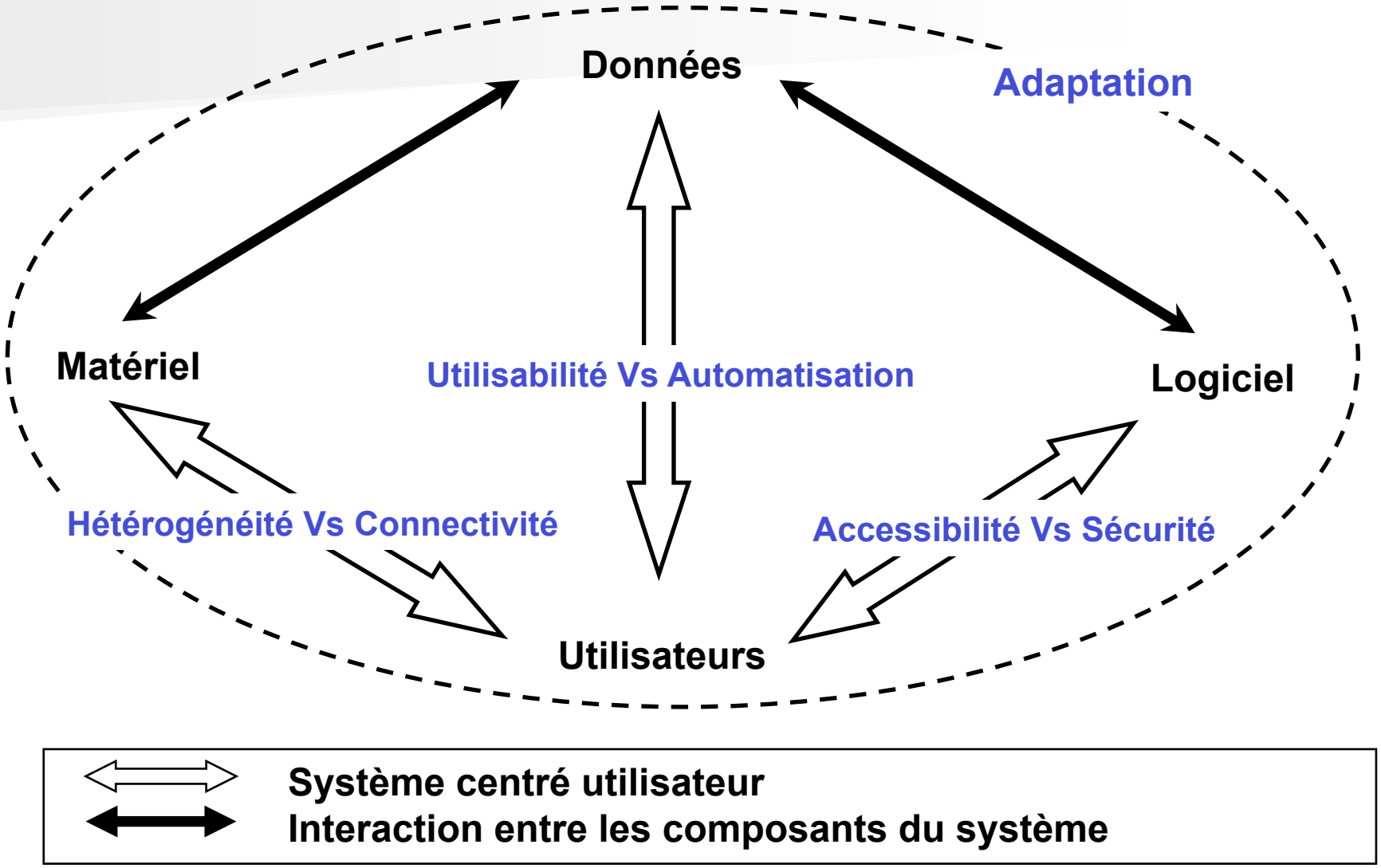
Introduction



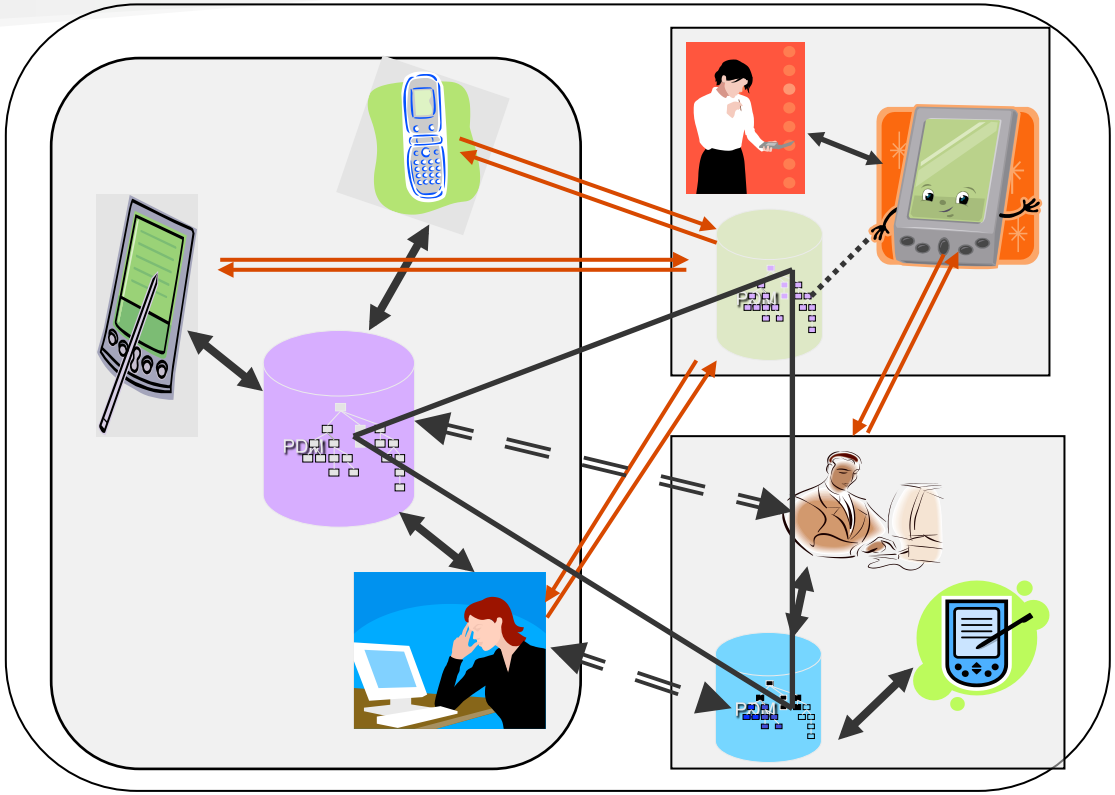
Définition

- Les Systèmes d'Information Pervasifs:
  - Visent à fournir un accès transparent aux ressources de données depuis:
    - N'importe où → (systèmes mobiles)
    - N'importe comment → (systèmes intelligents)
    - À n'importe quel moment → (systèmes au temps réel)

Les composants et challenges de SIP



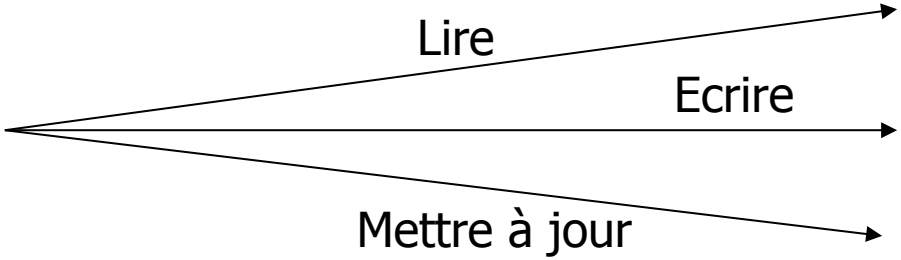
L'Accès aux données semi-structurées

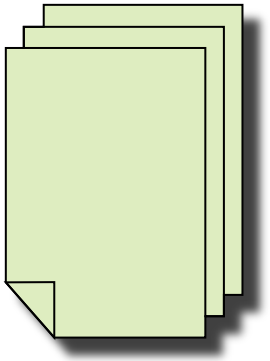


Accès direct aux données pour les utilisateurs du système local.
Accès indirect aux données externes (selon les droits d'accès).
Accès flots (données stockées sur des dispositifs mobiles).
Interaction visée (accessibilité directe à n'importe quel BD).

Le Contrôle d'accès

- La gestion d':
  - Un sujet (personne, processus informatique, machine, …)
  - Effectue une action (lire, écrire, mettre à jour, …)
  - Accéder une ressource (dossier, imprimante, …).





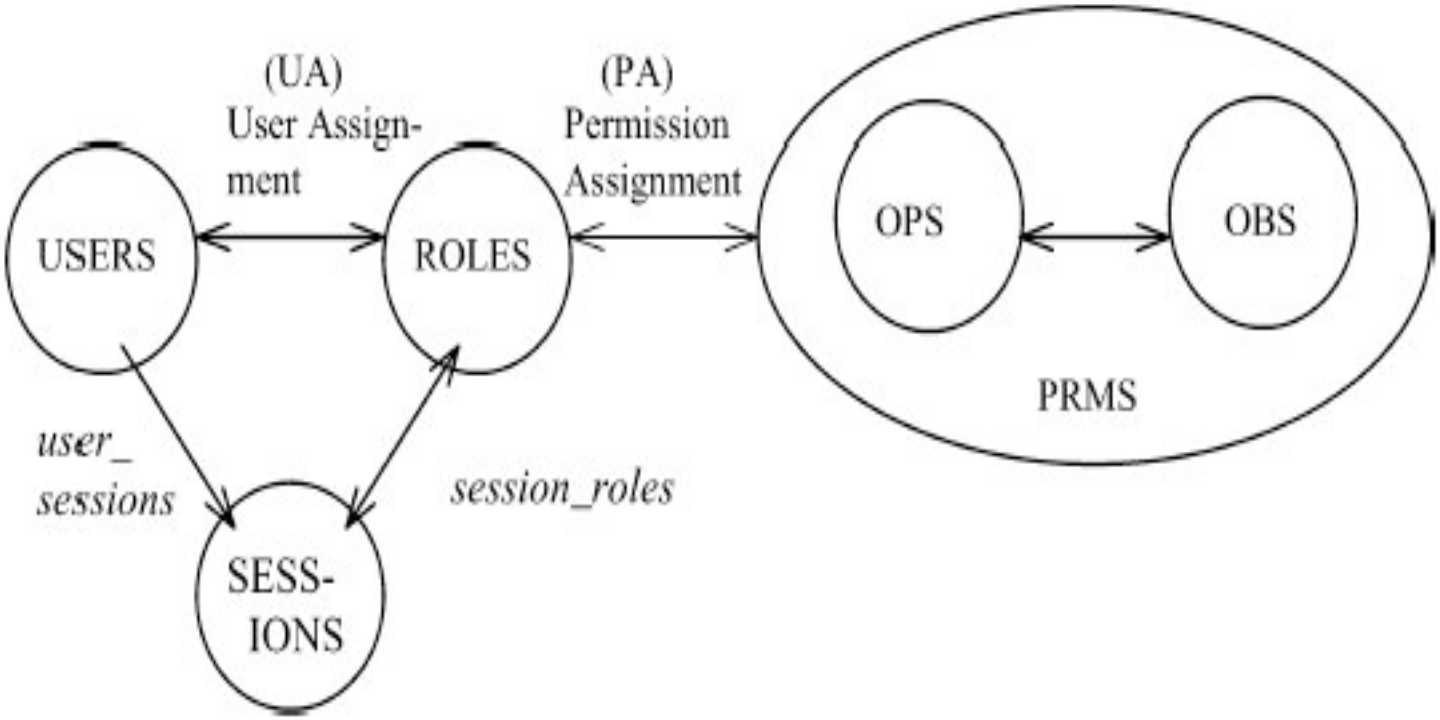
Sujet **Action** **Ressource**

Le Contrôle d'Accès & les systèmes d'informations

- Une grande nombre de personnes
- Une grande nombre de ressources (distribuées).
- Problème: Gestion des politiques d'accès
- Solutions:
  - Différents Modèles: DAC, MAC & RBAC.
    - RBAC: Role-Based Access Control
      - Il regroupe différentes utilisateurs du système selon leurs **rôle** dans l'hiérarchie de l'entreprise.
      - Il permet une **gestion décentralisée** dont les mis à jour d'une rôle peuvent être effectuées sans changer les permissions de chaque utilisateur.
      - Ce modèle est générique et a été supporté par beaucoup de systèmes informatiques.

RBAC Role Based Access Control

Ferraiolo et Kuhn, 1992



Les challenges d'expressivité des politiques du contrôle dans un environnement pervasif

- L'importance de prendre en compte le contexte dans un processus d'autorisation:

  - sa localisation.
  - sa machine (type, capacité, …)
  - Le réseau (débit, …)
  - Le temps.
  - …

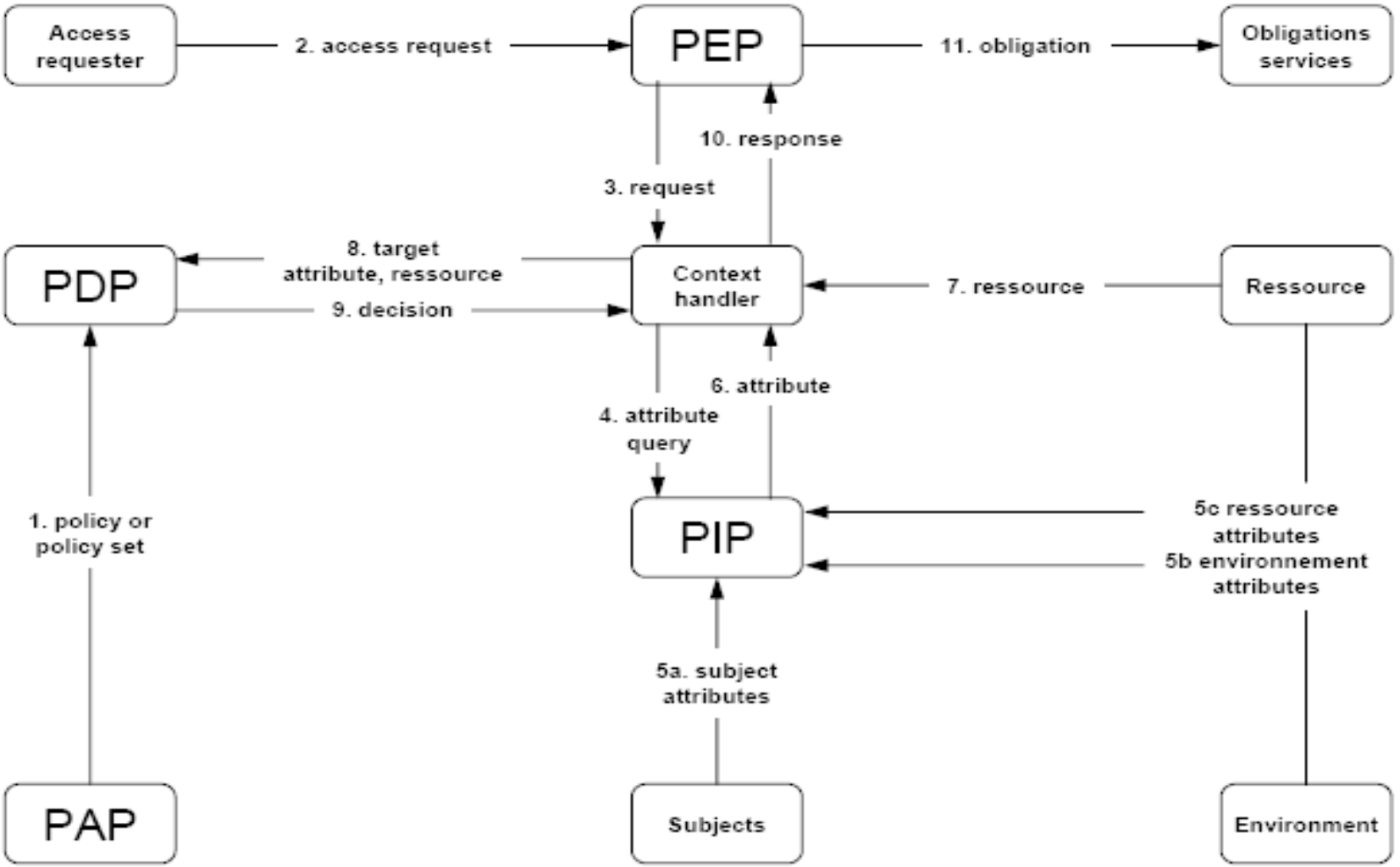
Le Contrôle d'Accès & l'évolution des systèmes d'informations pervasifs

- L'accès est plus compliqué:
  - Temps d'accès (T-RBAC)
  - Localisation d'accès (PAC, Geo-RBAC, uT-RBAC).
  - Environnement (DRBAC, Context Aware RBAC, ...)
- Objectif:
  - Accès à n'importe où, n'importe comment & à n'importe quel moment.
  - Décentralisation des ressources & droits d'accès.
  - Gestion centralisée pour l'accès aux ressources.

L'implémentation du Contrôle d'Accès dans l'âge des services web & documents semi-structurés

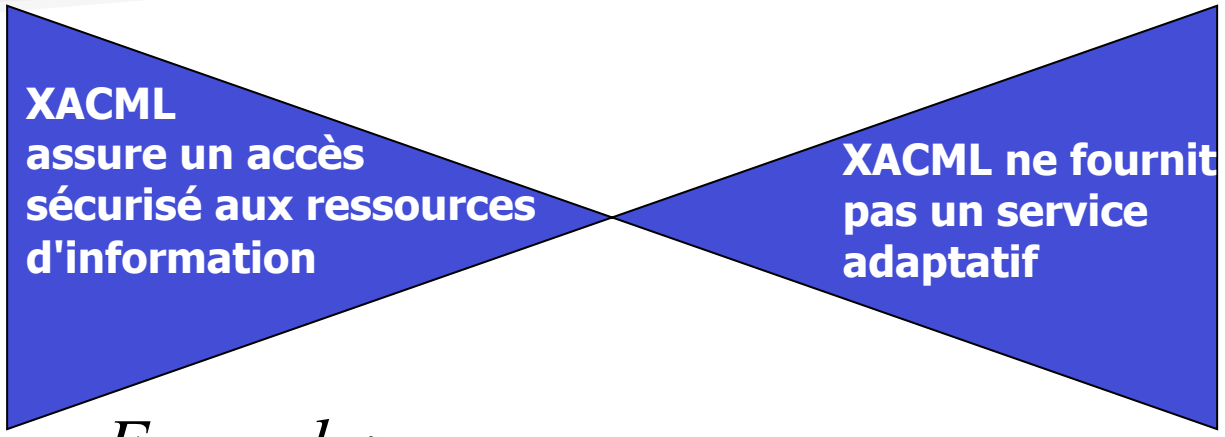
- XACML: eXtensible Access Control Markup Language
- Un langage qui :
  - ❖ Décrit des politiques de contrôle d'accès permettant de standardiser les décisions de contrôle d'accès aux documents XML.
  - ❖ Définit les privilèges des utilisateurs sur les ressources informatiques d'un système.
  - ❖ Permet d'authentifier et de sécuriser l'accès aux ressources d'information.
- Avantages:
  - Interopérable
    - Les règles de contrôle d'accès sont conservées dans un référentiel physiquement distinct du document.
  - Un langage expressive avec granularité fine.

XACML


Access requester
2. access request
PEP
11. obligation
Obligations services
10. response
3. request
PDP
8. target attribute, ressource
9. decision
Context handler
7. ressource
Ressource
6. attribute
4. attribute query
1. policy or policy set
PIP
5c ressource attributes
5b environnement attributes
5a. subject attributes
PAP
Subjects
Environment

XACML et La Qualité de Service

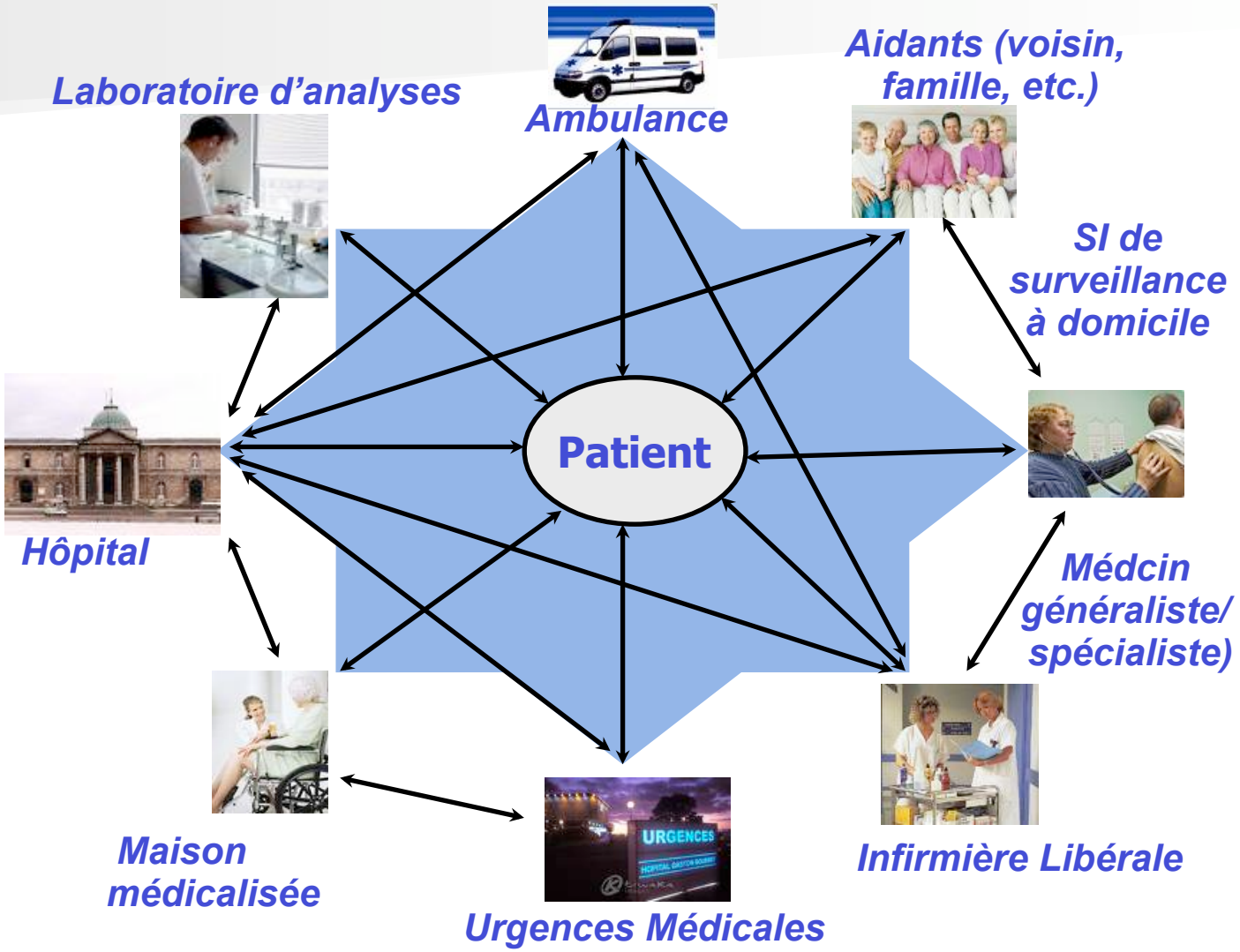
Point de vue du système **Perspective de l'utilisateur**



Exemple:

- **La demande de l'utilisateur :**
  - ❖ L'accès à un objet non-autorisé d'un document.
- **Réponse du système:**
  - ❖ Il rejette sa demande au lieu d'afficher une sous-partie autorisée de l'arbre.
  - ❖ **Manque d'adaptivité**

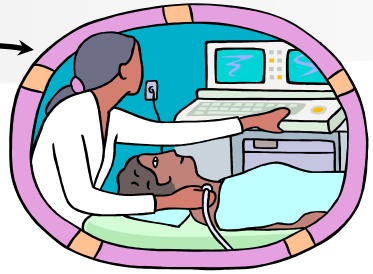
Application Pervasive: les Systèmes de Santé



1. Système Centralisé au Client (Patient, médecin,…).
2. Distribués aux différents sources.
3. Traitement de données est en temps réel.
4. Accès aux données multimédia depuis dispositif mobile).
5. La Gestion et la prise de décision centralisée.

Etude de Cas: Scénario d'urgence

Urgence

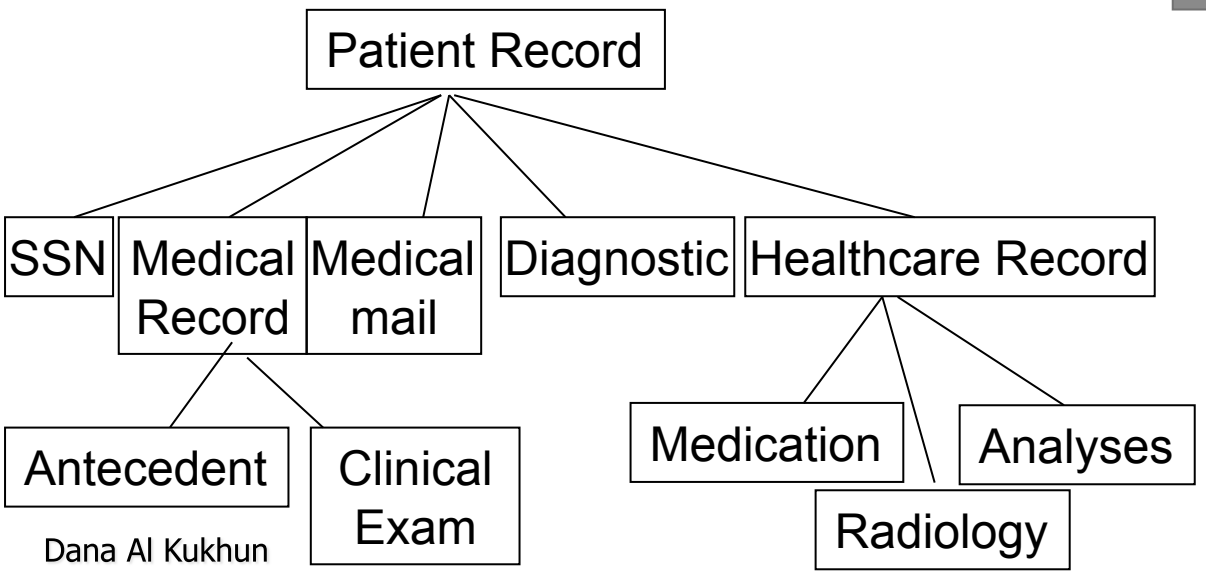


consultation Mobile

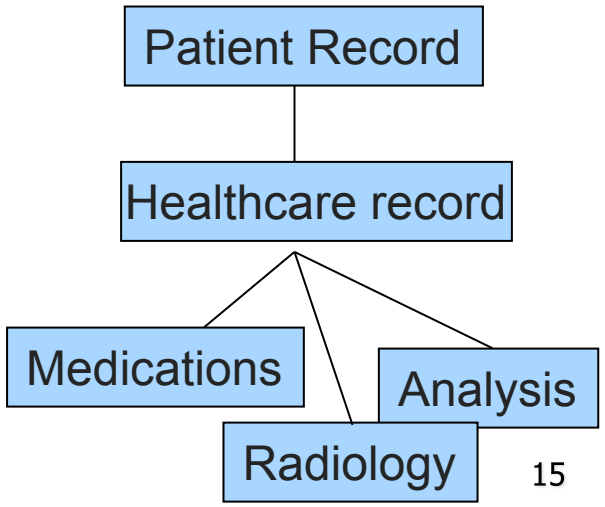
Access au dossier de patient

Problem: restrictions d'accès à cause du profile RBAC

Doctor View



Nurse View



L'adaptation du Contrôle d'Accès

- Malgré la variation des contraintes du temps réel, l'utilisateur a toujours besoin d'accéder le système.
  - Spécialement dans les cas critiques (Urgence, incendie, blocage du système, etc).
- Notre proposition vise à:
  - Respecter les règles & les droits d'accès
  - Donner aux utilisateurs des informations pertinentes & utiles selon leur(s):
    - **Privilèges**.
    - **Situation contextuelle (cas critique).**
    - **Contexte (localisation, temps, connectivité).**

Plan

- Introduction
- Problématique
- État de l'art
- Proposition
  - Un Modèle Adaptable de RBAC.
  - Méthodologie: La réécriture des requêtes XACML.
- Conclusion et Perspectives

Solution:

La réécriture de requêtes XACML

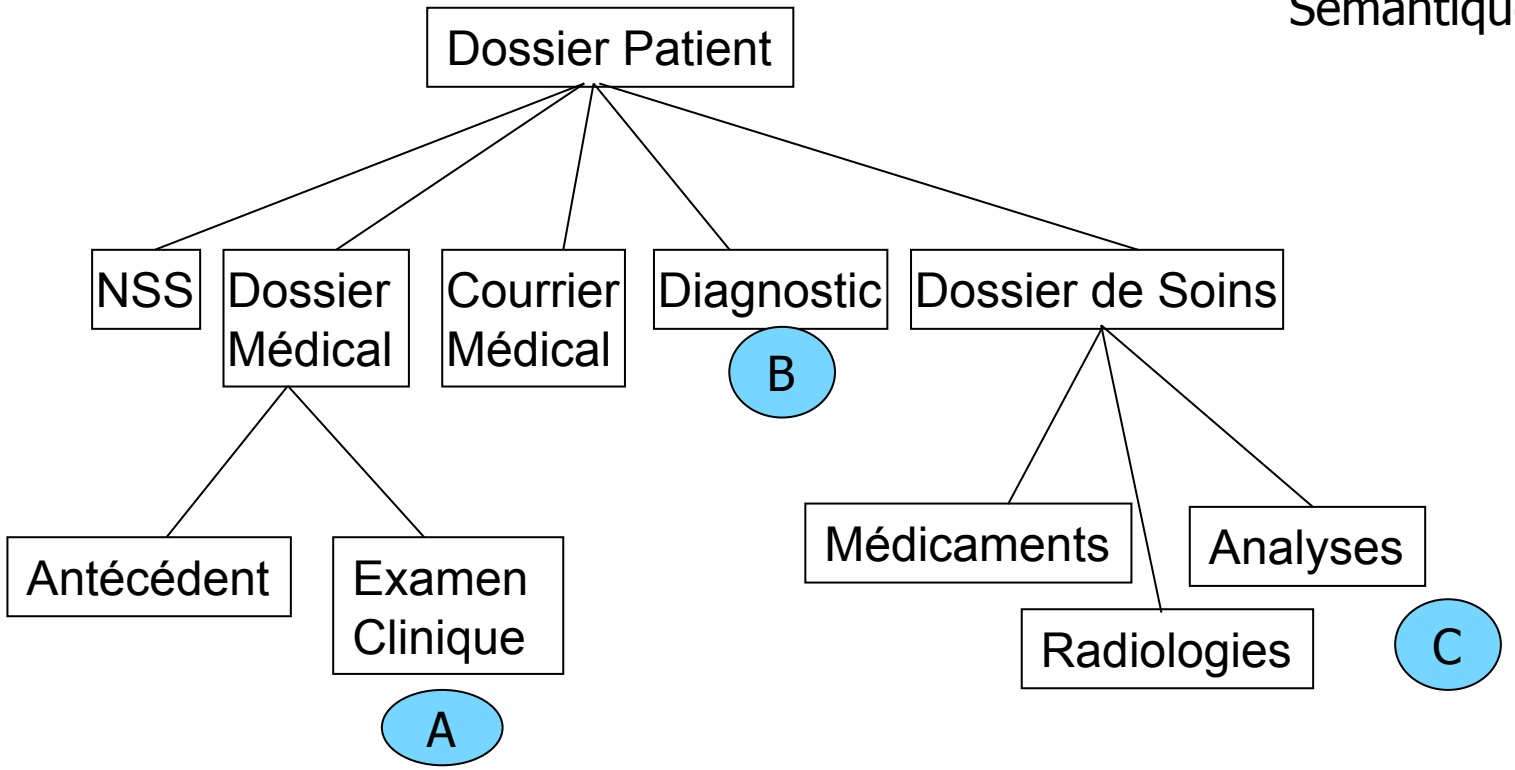
- Un mécanisme adaptable qui permet de:
  - ❖ Récupérer la plus grande quantité d'information disponible.
  - ❖ En utilisant des vues virtuelles qui changent la structure d'un document
    - En fonction
      - ❖ du rôle de l'utilisateur
      - ❖ son contexte (temps, localisation, connectivité)
      - ❖ de similarité entre les différents éléments d'un document.

      ➔ Sans menacer la sécurité ou l'intégrité du système.

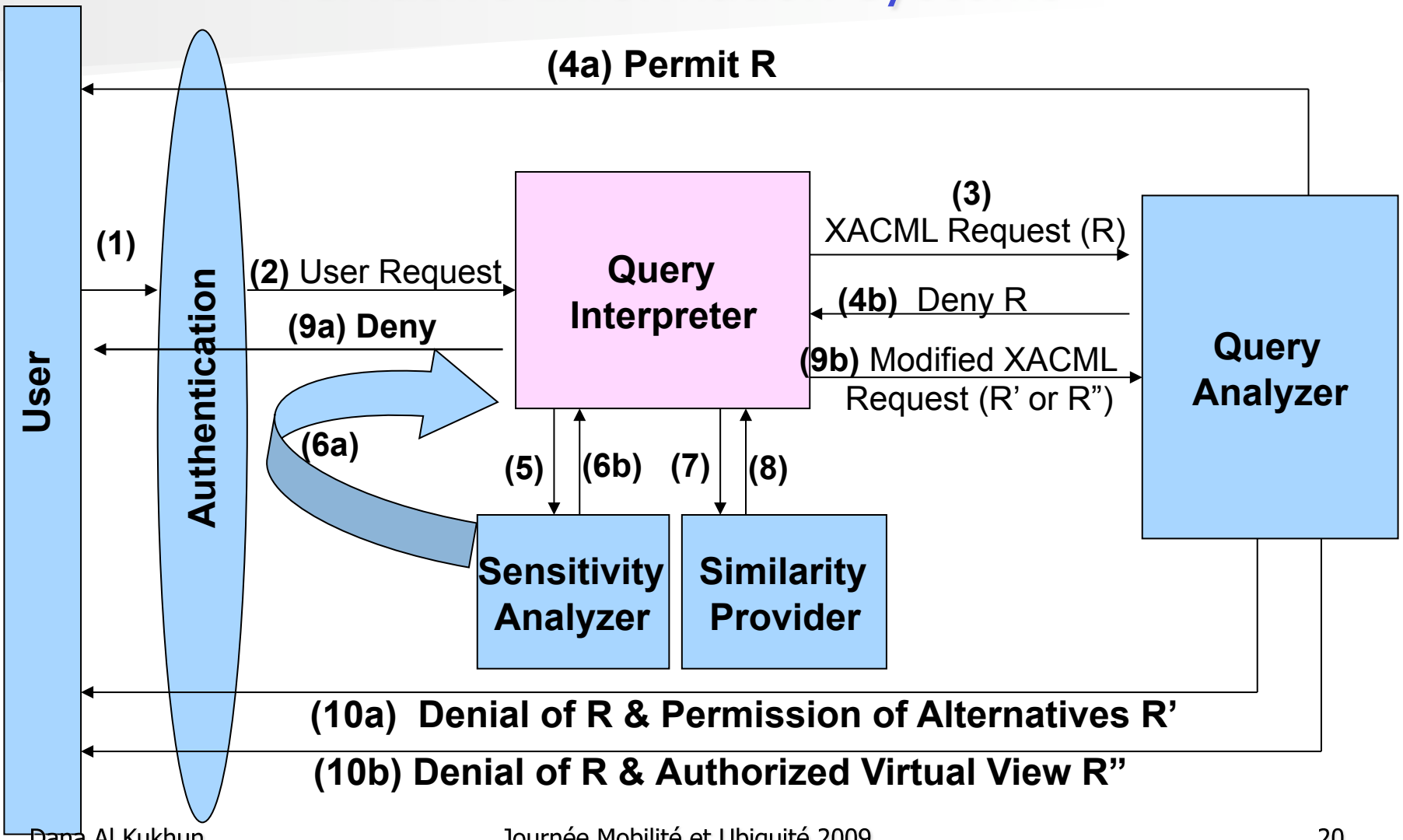
Démonstration

Role	E1	E2	Sim (E1,E2)
Docteur	B	A	0.90
Infermière	A	B	0.00 → Pas droit
Infermière	A	C	0.80

Sémantique



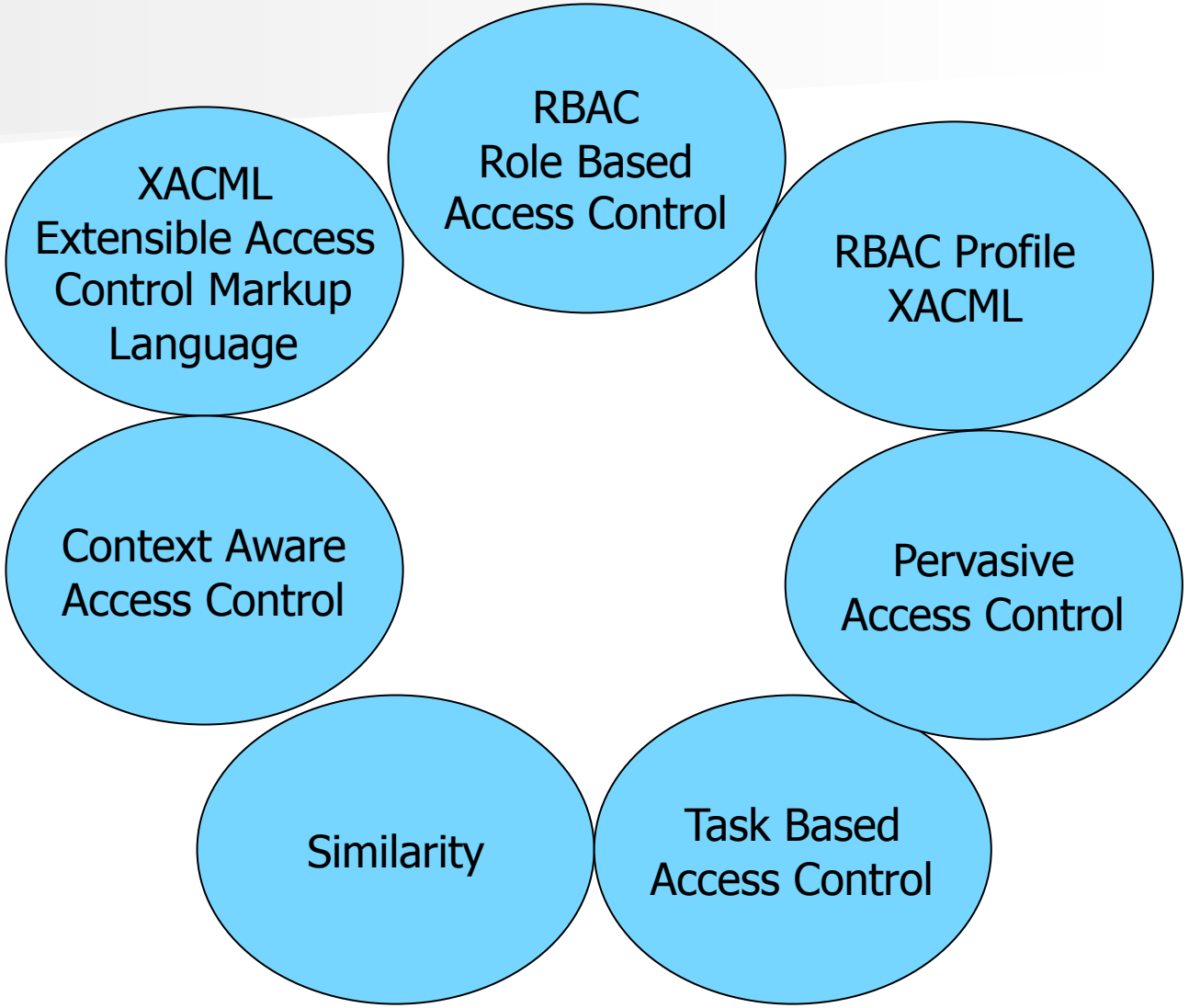
MAAC-PIS: Mutually Adaptive Access Control for Pervasive Information Systems



Plan

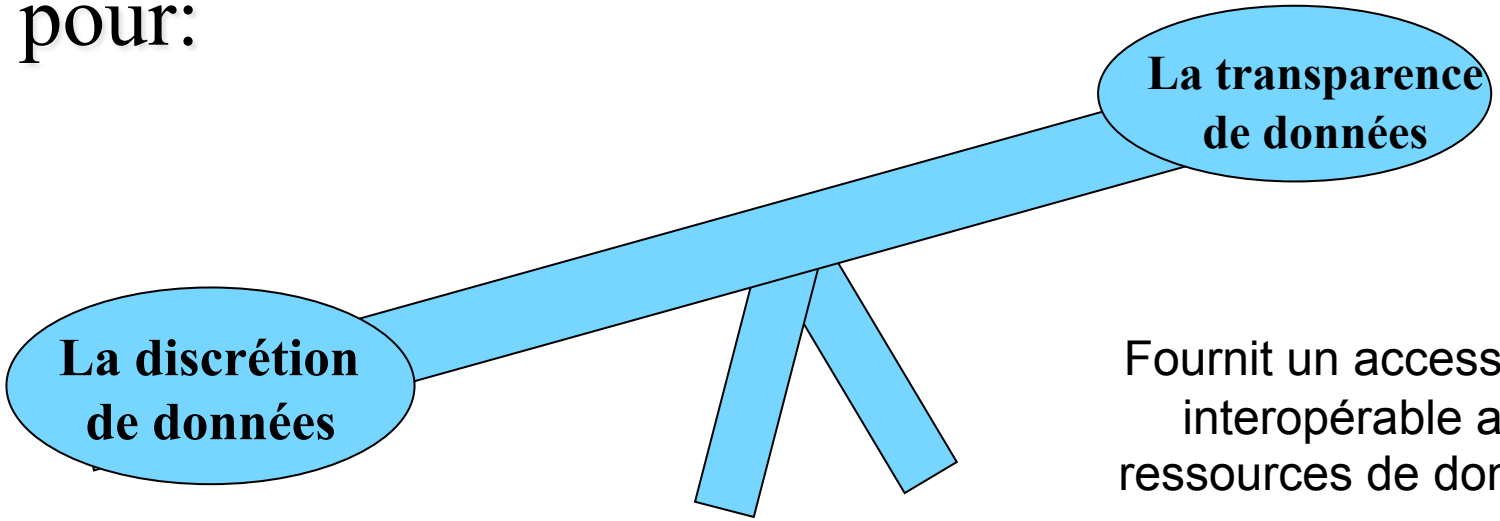
- Introduction
- Problématique
- État de l'art
- Proposition
- Conclusion et Perspectives

Une étape en avance



Conclusion

- Notre objectif est d'appliquer l'adaptation pour:

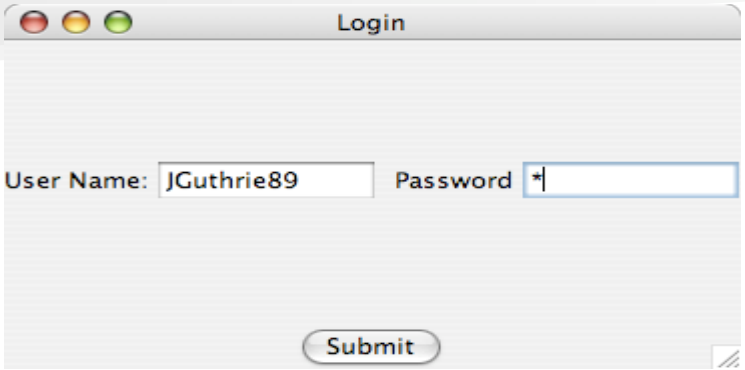


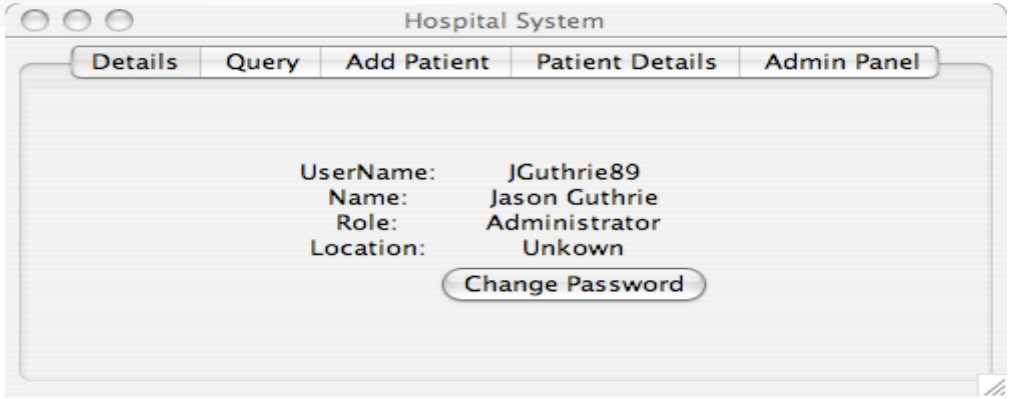
Fournit un accessibilité interopérable aux ressources de données

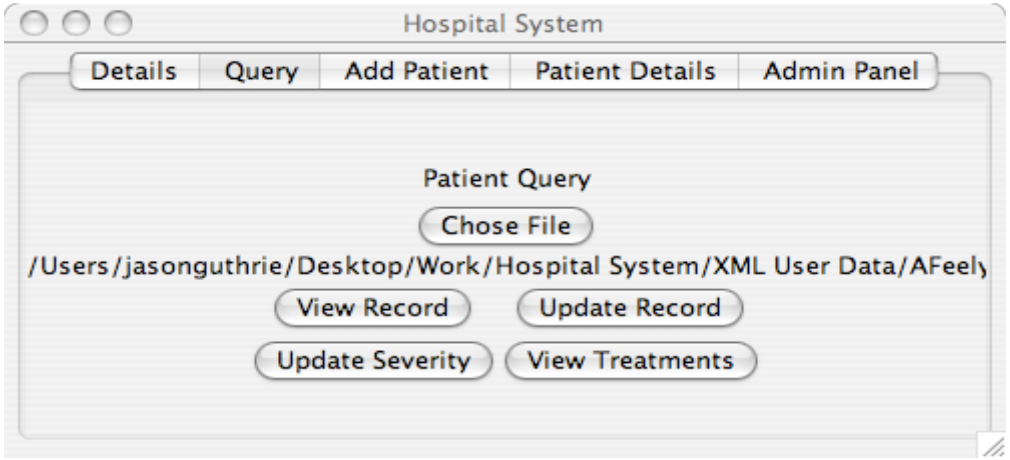
Minimise leur vulnérabilité aux attaques de sécurité.

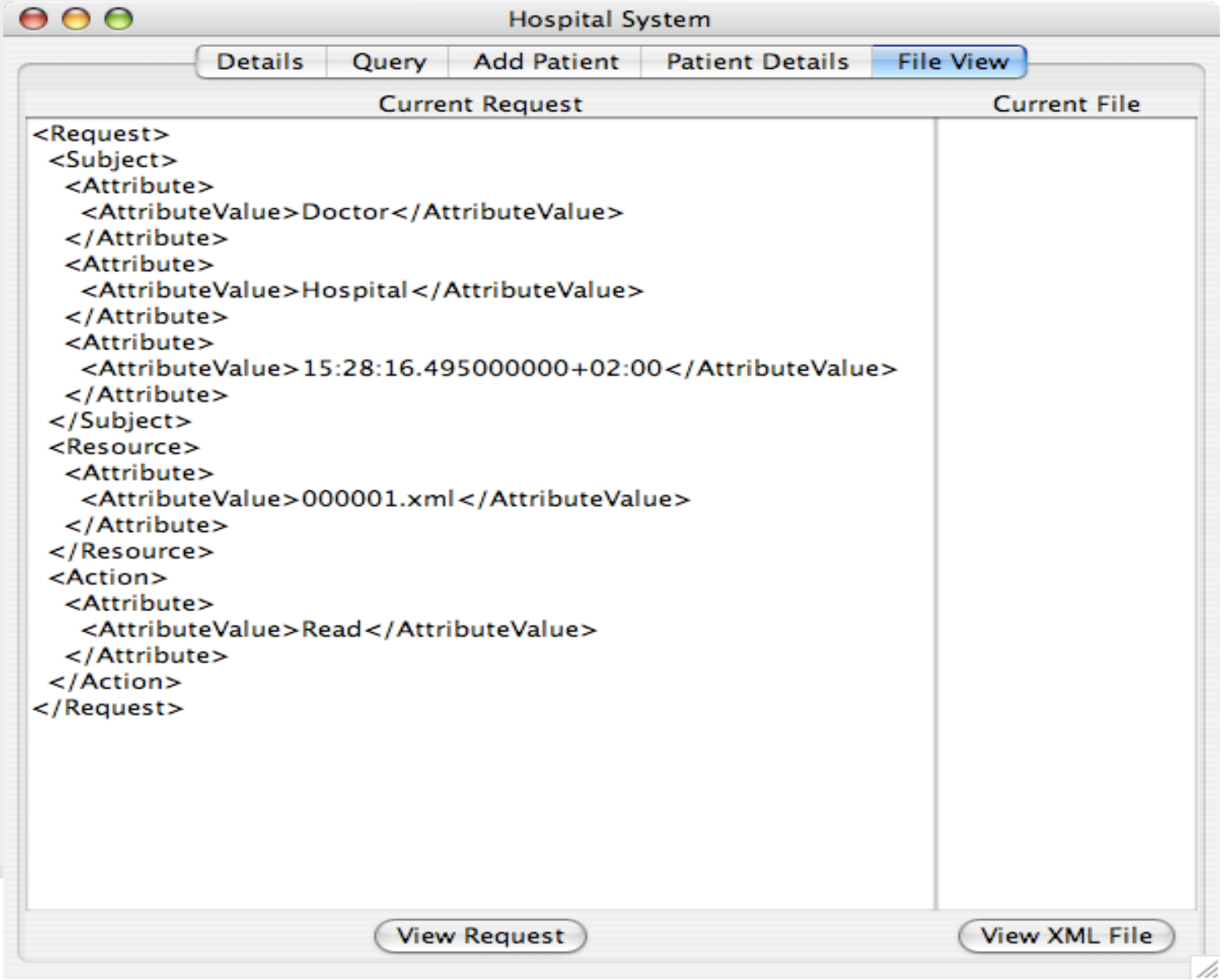
Merci de votre attention

Fonctionnement du Système








Hospital System
Details
Query
Add Patient
Patient Details
File View
Current Request
Current File
<Request>
<Subject>
<Attribute>
<AttributeValue>Doctor</AttributeValue>
</Attribute>
<Attribute>
<AttributeValue>Hospital</AttributeValue>
</Attribute>
<Attribute>
<AttributeValue>15:28:16.495000000+02:00</AttributeValue>
</Attribute>
</Subject>
<Resource>
<Attribute>
<AttributeValue>000001.xml</AttributeValue>
</Attribute>
</Resource>
<Action>
<Attribute>
<AttributeValue>Read</AttributeValue>
</Attribute>
</Action>
</Request>
View Request
View XML File

Un Exemple d'une Requête

```
<?xml version="1.0" encoding="UTF-8"?>
<Request
    xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
     access_control-xacml-2.0-context-schema-os.xsd">
  <Subject>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>Doctor</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>http://medico.com/record/patient/BartSimpson/eye_exam</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>read</AttributeValue>
    </Attribute>
  </Action>
  <Environment/>
</Request>
```

Un Exemple d'une Politique

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
    xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
      access_control-xacml-2.0-policy-schema-os.xsd"
    PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA1:policy"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
      algorithm:deny-overrides">
<Target/>
  <Rule
      RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA1:rule"
      Effect="Permit">
<Target>
        <Subjects>
          <Subject>
            <SubjectMatch
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType=
      http://www.w3.org/2001/XMLSchema#string>Doctor</AttributeValue>
              <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </SubjectMatch>
          </Subject>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
              <AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://
      medico.com/record/patient/BartSimpson/eye_exam</AttributeValue>
              <ResourceAttributeDesignator
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
            </ResourceMatch>
          </Resource>
        </Resources>
<Actions>
          <Action>
            <ActionMatch
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue     DataType="http://www.w3.org/2001/
      XMLSchema#string">read</AttributeValue>
              <ActionAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ActionMatch>
          </Action>
          <Action>
            <ActionMatch
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue                    DataType="http://www.w3.org/
      2001/XMLSchema#string">write</AttributeValue>
              <ActionAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ActionMatch>
          </Action>
        </Actions>
      </Target>
  </Rule>
</Policy>
```

Un Exemple d'une Réponse

```
<?xml version="1.0" encoding="UTF-8"?>
<Response
    xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:
    2.0:context:schema:osaccess_control-xacml-2.0-context-
    schema-os.xsd">
   <Result>
      <Decision> Permit</Decision>
      <Status>
         <StatusCode
              Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
      </Status>
   </Result>
</Response>
```