Exercise 05:
LPL, Access control, Policy enforcement & XACML

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

Task 1:
LPL

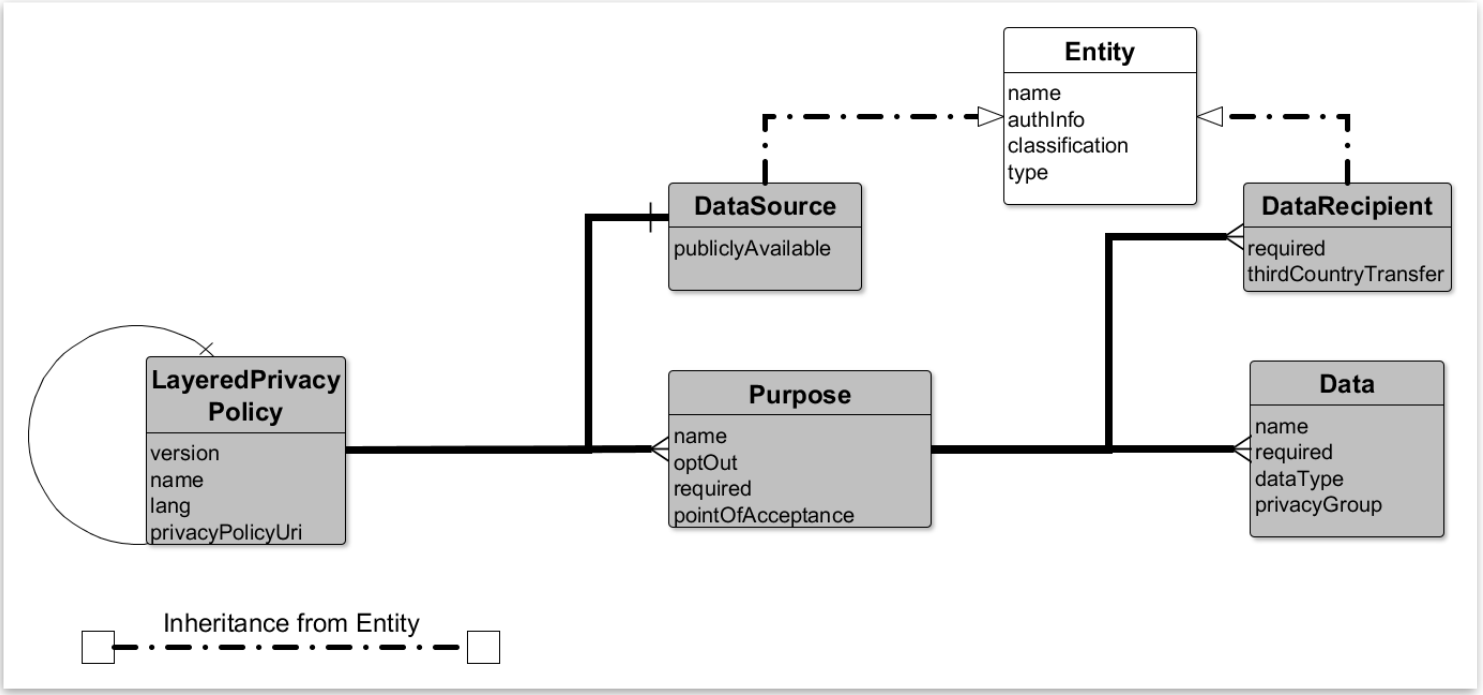
Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

LPL

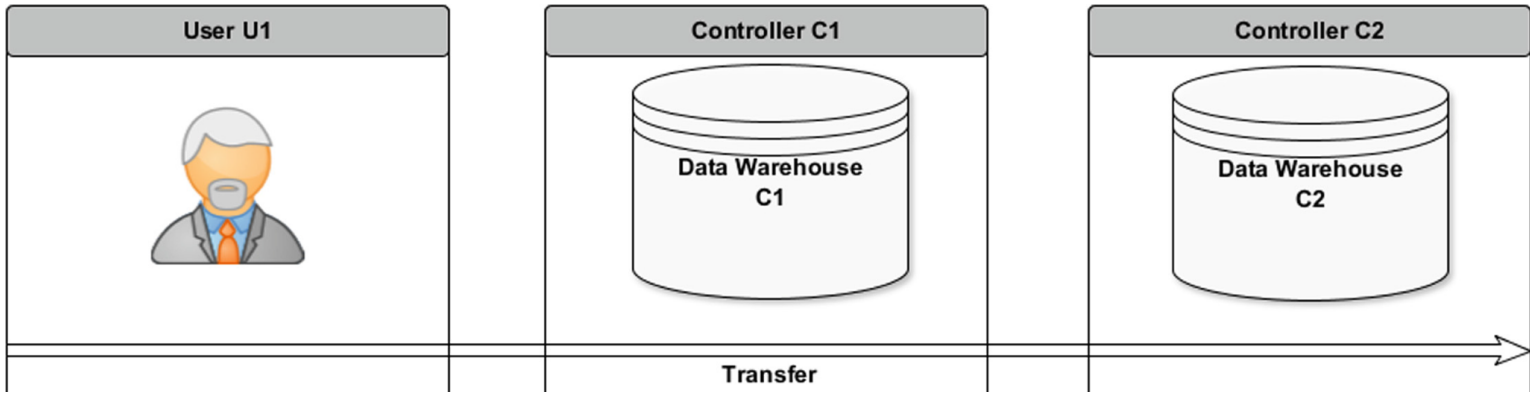
L: Layered **P**: Privacy **L**: Language



LPL core structure

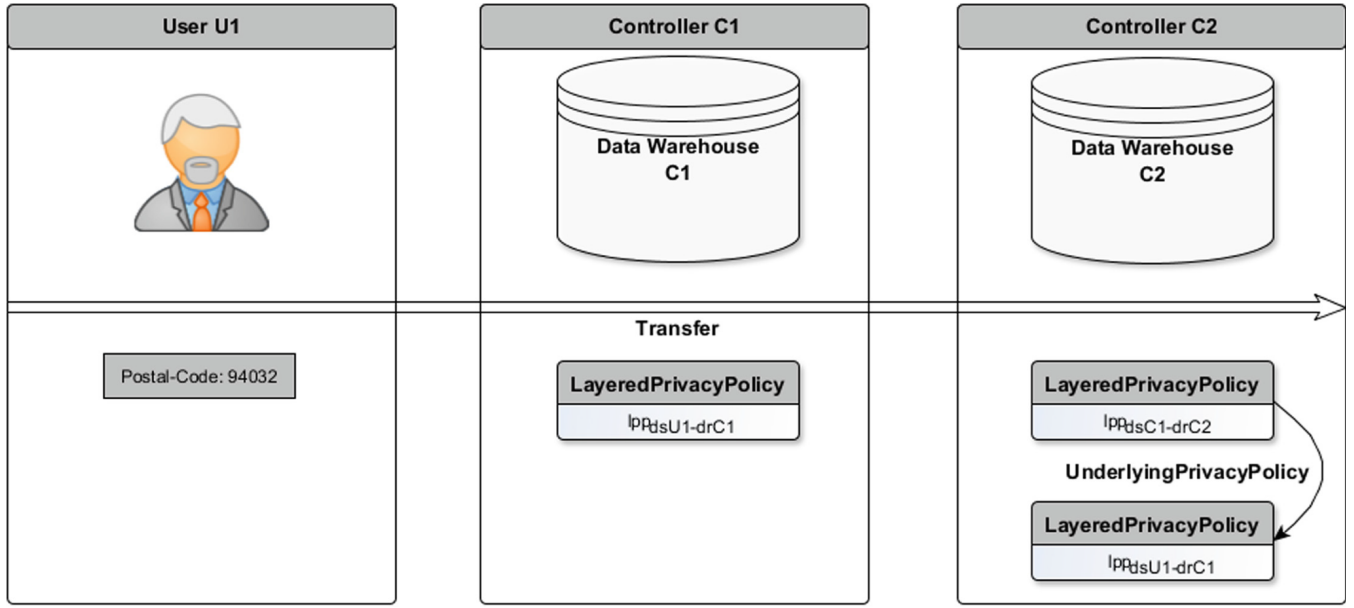
Category Provenance

- Data Subject has to be **identifiable** (to claim his/her DSR) even after personal data is **transferred** from **one Controller** to **another**.



Category Provenance in LPL

- LayeredPrivacyPolicy can reference other LayeredPrivacyPolicy-element
  - **UnderlyingPrivacyPolicy**



De-identification in LPL

De-identification mechanisms

- Pseudonymization
  - **PseudonymizationMethod** defines Method
  - **NameOfData** defines target Attribute
- Personal Privacy Anonymization (Localized Anonymization)
  - **AnonymizationMethod** defines Method for **Data**
  - E.g., Suppression, Generalization, Deletion, etc.
- Privacy Model (Data-Set)
  - **PrivacyModel** defines Method
  - E.g., k-Anonymity, l-Diversity, etc.

Task 2:
Access control

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

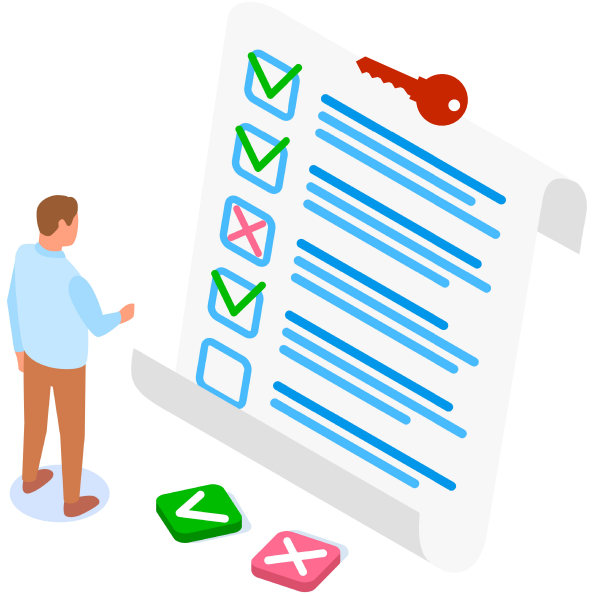
WS 21/22

Authorisation vs. Authentification

- Two fundamental aspects of privacy
- **Authentication** is a technique used to verify that the user is who they claim to be.
- Authentication isn’t sufficient by itself to protect data.
- **Authorization** is needed to determine whether a user should be allowed to access the data and what functions is permitted to carry out.

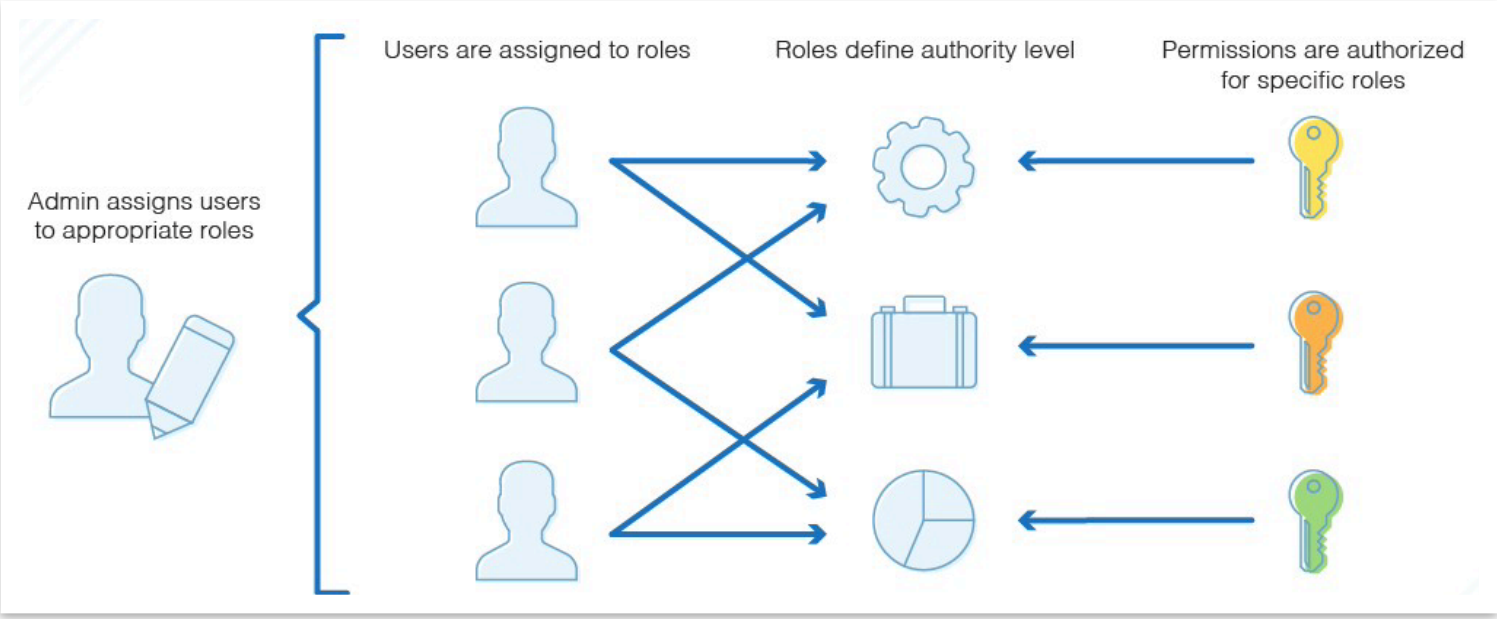
ACL (Access Control List)

- Access control lists are permission-based service that assign user different levels of access to data.



RBAC (Role-Based Access Control)

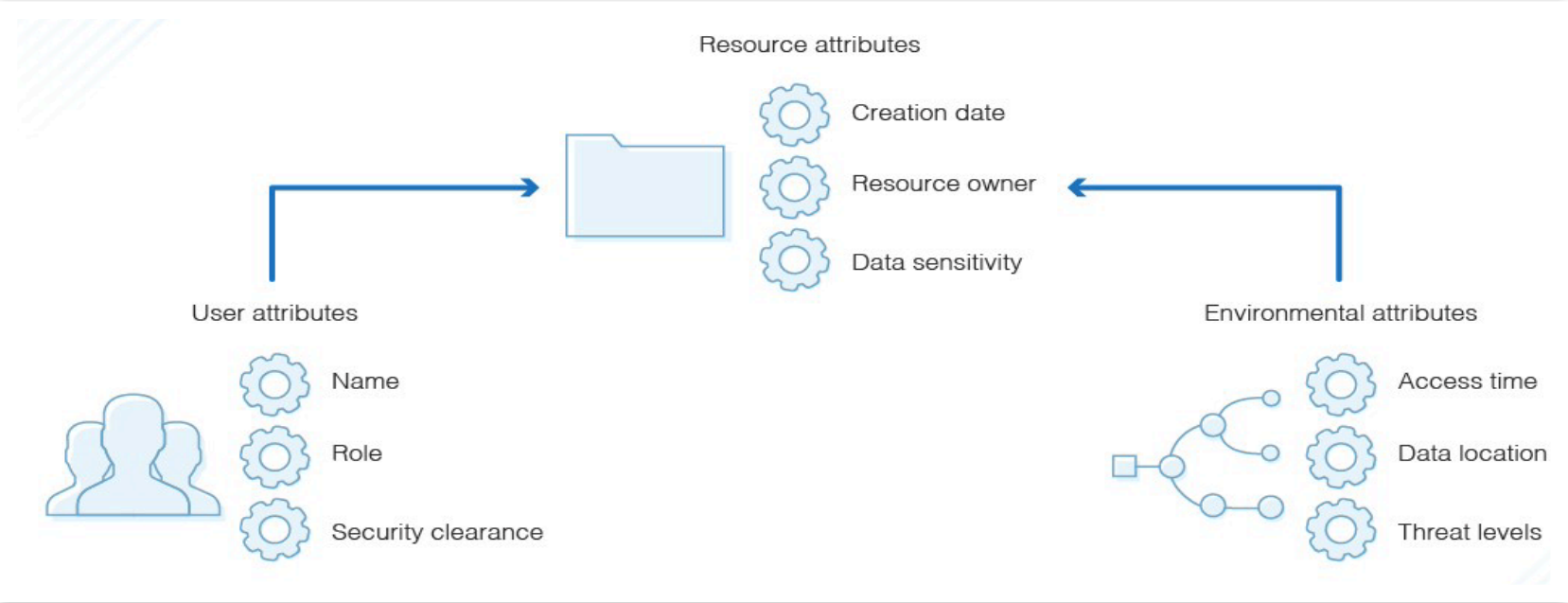
- Provides access to data based on user **roles**.



Source: https://www.dnsstuff.com/rbac-vs-abac-access-control

ABAC (Attribute-Based Access Control)

- Provides access rights based on user, environment, or resource attributes.
- ABAC has a much greater number of possible control variables than RBAC.
- ABAC is the more complex, requiring more processing power and time.



Source: https://www.dnsstuff.com/rbac-vs-abac-access-control

Task 3:
XACML

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

XACML Policy — Server “SampleServer”

```
<Policy PolicyId="SamplePolicy"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">

  <!-- This Policy only applies to requests on the SampleServer -->
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer</AttributeValue>
        <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
      </ResourceMatch>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
</Policy>
```

XACML Policy — Rule

```
<!-- Rule to see if we should allow the Subject to login -->
<Rule RuleId="LoginRule" Effect="Permit">

  <!-- Only use this Rule if the action is login -->
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <AnyResource/>
    </Resources>
    <Actions>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">login</AttributeValue>
        <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                   AttributeId="ServerAction"/>
      </ActionMatch>
    </Actions>
  </Target>
</Rule>
```

XACML Policy — Rule & Condition

```
<!-- Only allow logins from 9am to 5pm -->
<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal"
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
      <EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"
                                    AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>
    </Apply>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
  </Apply>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal"
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
      <EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"
                                    AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>
    </Apply>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
  </Apply>
</Condition>
```

XACML Policy — Example

```
Policy PolicyId="SamplePolicy"
       RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">

  <!-- This Policy only applies to requests on the SampleServer -->
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer</AttributeValue>
        <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
      </ResourceMatch>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>

  <!-- Rule to see if we should allow the Subject to login -->
  <Rule RuleId="LoginRule" Effect="Permit">

    <!-- Only use this Rule if the action is login -->
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">login</AttributeValue>
          <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                     AttributeId="ServerAction"/>
        </ActionMatch>
      </Actions>
    </Target>

    <!-- Only allow logins from 9am to 5pm -->
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal"
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
          <EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"
                                        AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>
        </Apply>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
      </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal"
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
          <EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"
                                        AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>
        </Apply>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
      </Apply>
    </Condition>

  </Rule>

  <!-- We could include other Rules for different actions here -->

  <!-- A final, "fall-through" Rule that always Denies -->
  <Rule RuleId="FinalRule" Effect="Deny"/>

</Policy>
```

See you next week ☺