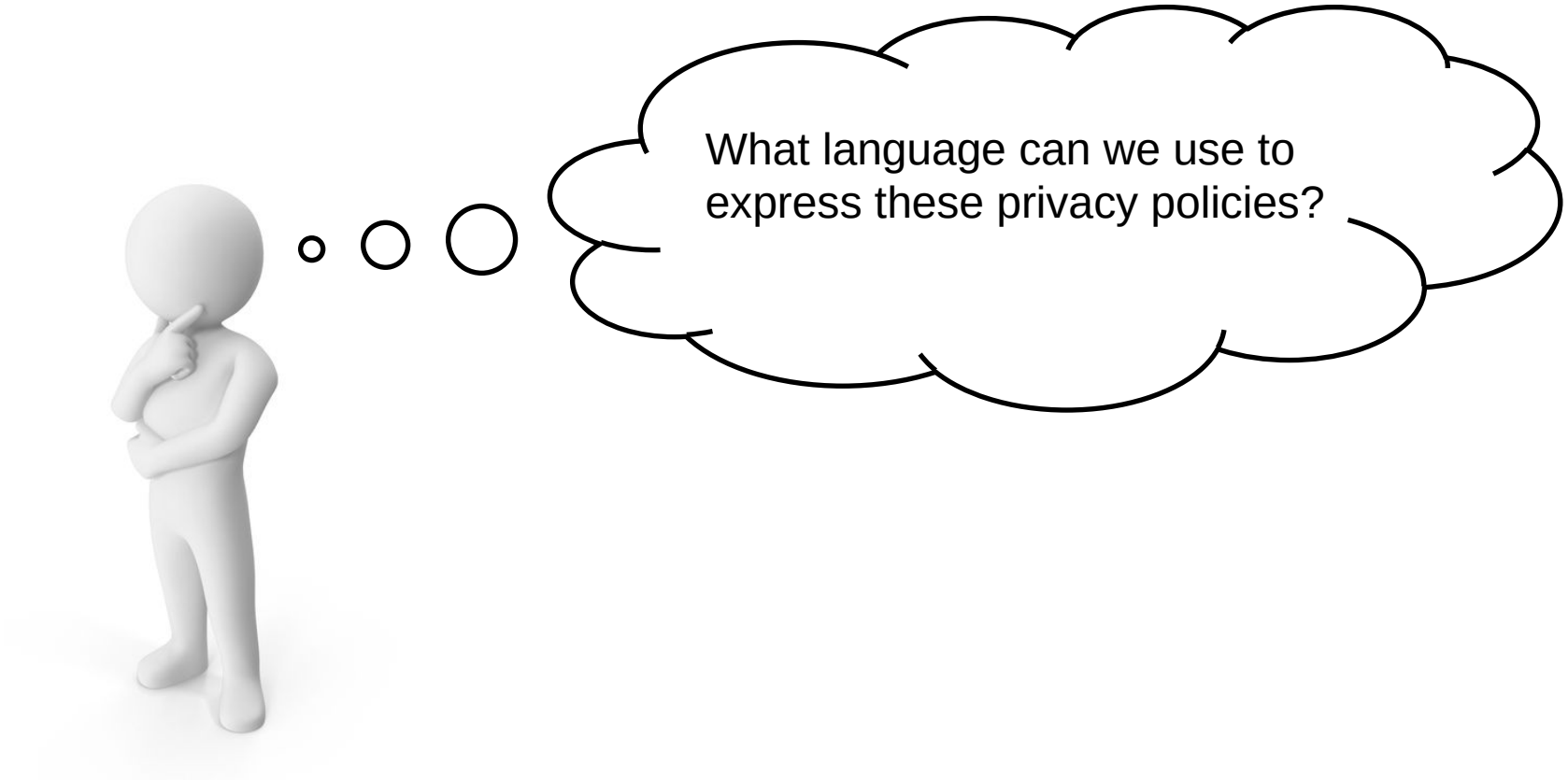
Towards time privacy policies in ODRL

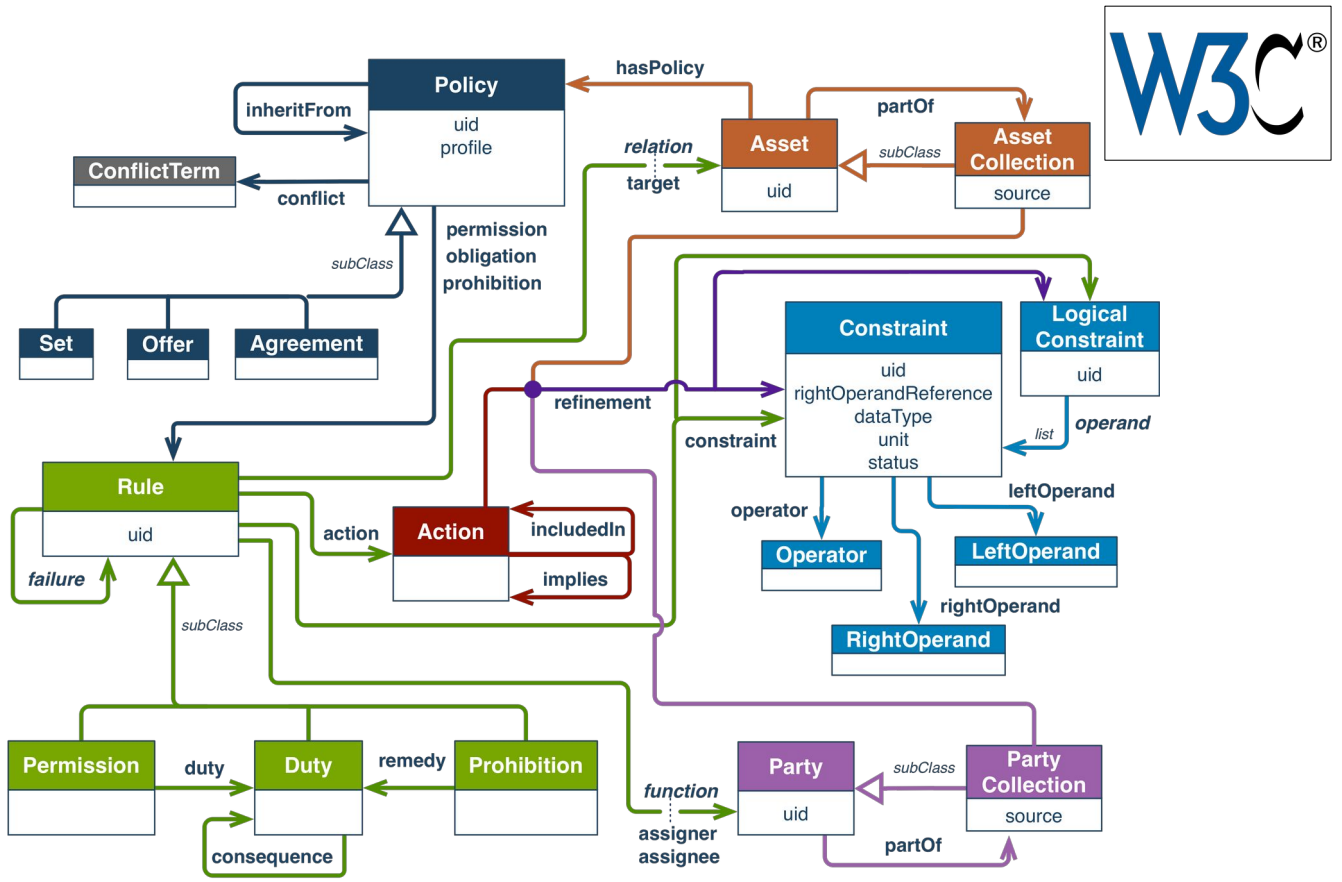
Juan Cano de Benito, Andrea Cimmino, Raúl García-Castro
Ontology Engineering Group
Universidad Politécnica de Madrid
Spain

juan.cano@upm.e @jucanbe 17/09/2024 Amsterdam

- The digital world has over 20 billion IoT devices.
- Information of IoT devices can be highly sensitive.
- Users need to incorporate certain privacy policies.



- Privacy policies can be expressed through the Open Digital Rights Language (ODRL) language.
- ODRL is a W3C open standard designed to express and communicate digital rights policies in a standardised way.



Why extend ODRL?

- ODRL language is a high-level vocabulary and therefore has limitations in representing domain-specific policies.
- Due to the large number of different IoT devices, ODRL needs to be extended.


```
{
  "@context":"http://www.w3.org/ns/odrl.jsonld",
  "@type":"Offer",
  "uid":"http://example.com/policy:9090",
  "profile":"http://example.com/odrl:profile:07",
  "permission":[
    {
      "target":"http://example.com/game:9090",
      "assigner":"http://example.com/org:xyz",
      "action":"play",
      "constraint":[
        {
          "leftOperand":"dateTime",
          "operator":"lt",
          "rightOperand":{
            "@value":"2017-12-31",
            "@type":"xsd:date"
          }
        }
      ]
    }
  ]
}
```

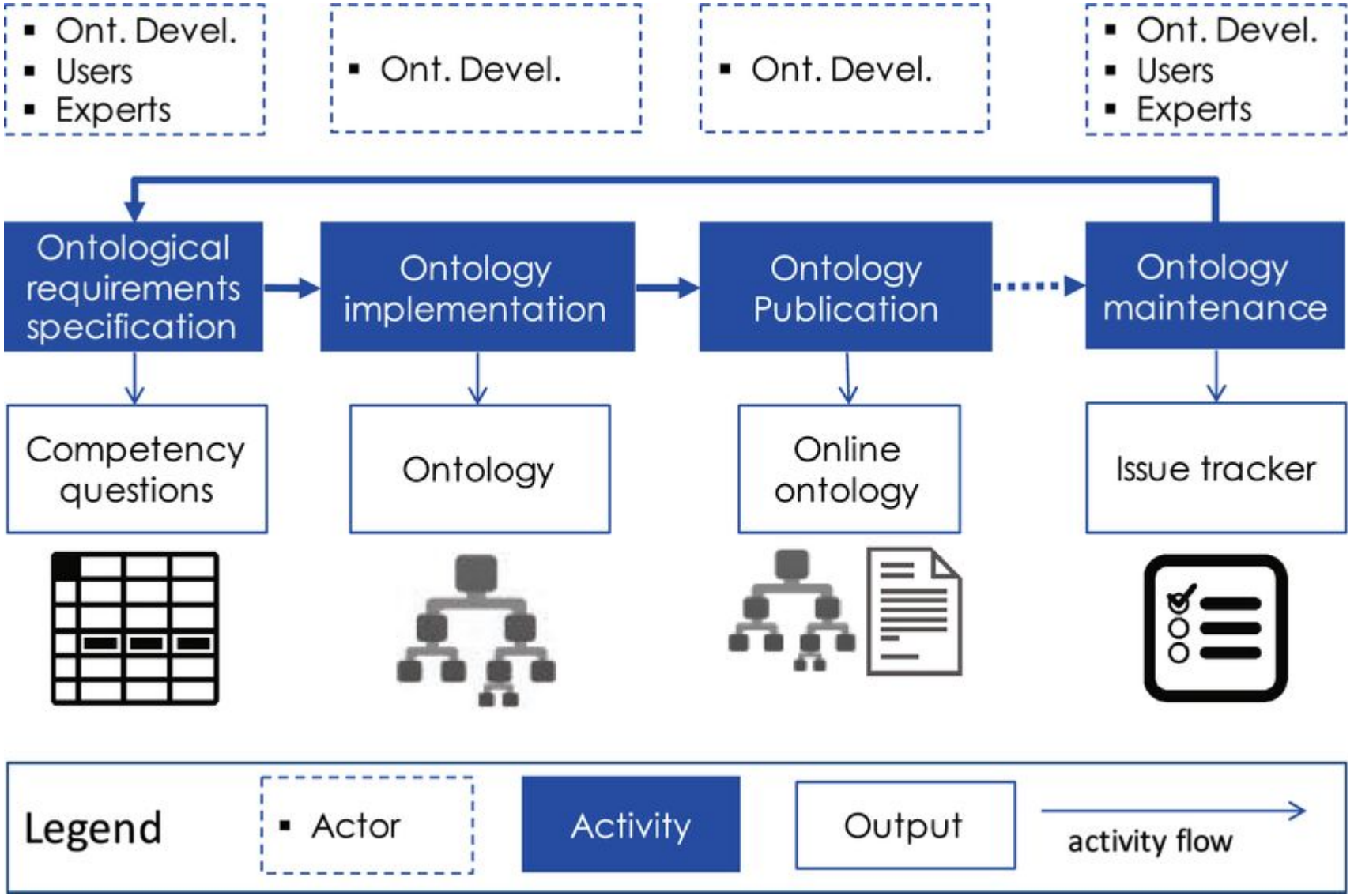
- ODRL presents certain limitations:
  - Ontological level. For example, “Greater Than” and “Less Than” of the ODRL ontology are not specified to handle dates.
  - Implementation specification (enforcement). ODRL does not provide an implementation specification.
  - Limitations in the expressiveness (enforcement). The ODRL specification is not detailed enough on how the policies are evaluated by a software system.

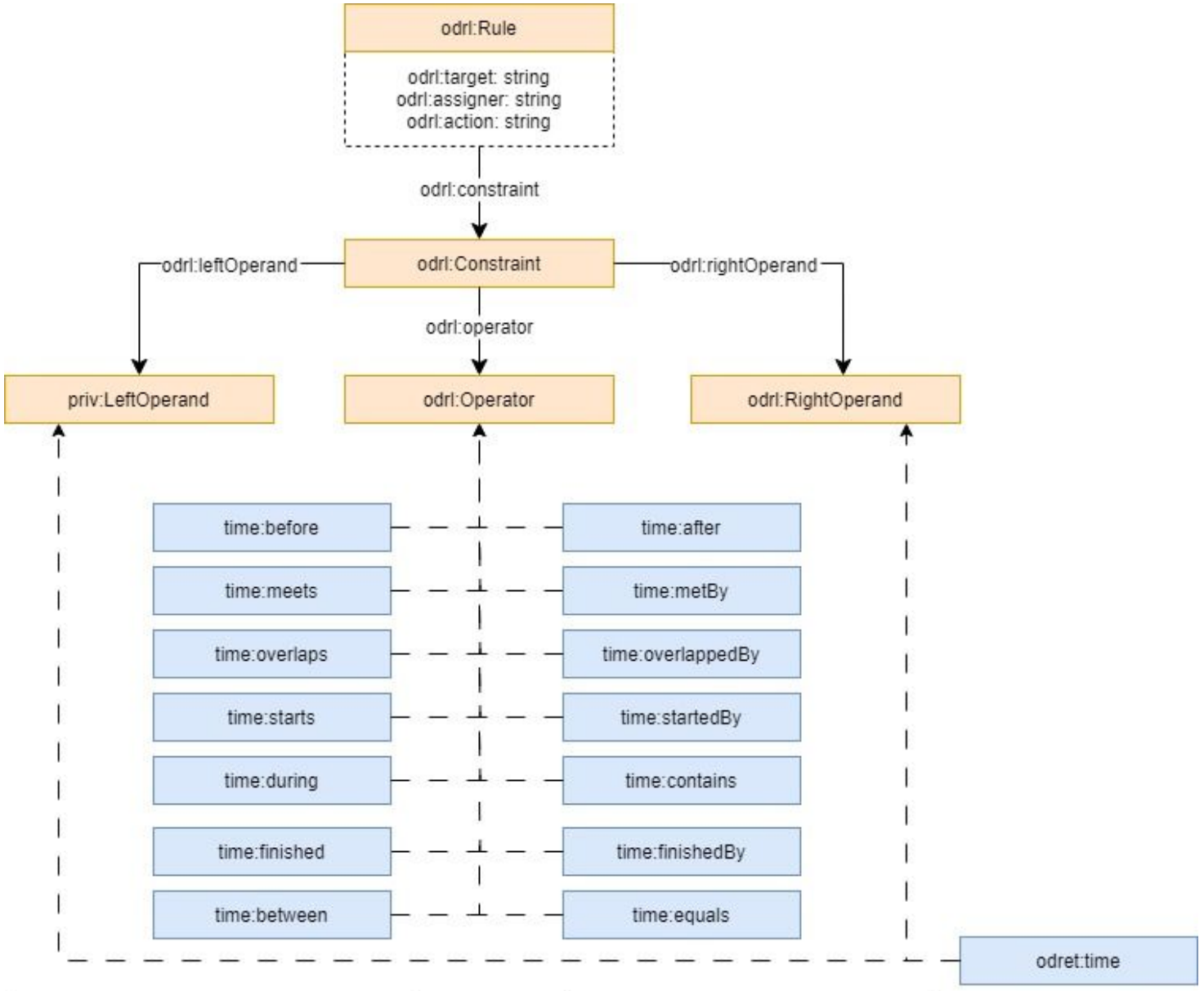
```
{
  "@context":"http://www.w3.org/ns/odrl.jsonld",
  "@type":"Offer",
  "uid":"http://example.com/policy:9090",
  "profile":"http://example.com/odrl:profile:07",
  "permission":[
    {
      "target":"http://example.com/game:9090",
      "assigner":"http://example.com/org:xyz",
      "action":"play",
      "constraint":[
        {
          "leftOperand":"dateTime",
          "operator":"lt",
          "rightOperand":{
            "@value":"2017-12-31",
            "@type":"xsd:date"
          }
        }
      ]
    }
  ]
}
```

- One of the current limitations is the ontological level.
  - The ODRL ontology is high-level
    - Operators like "greater than" or "less than" are specified from this high-level perspective.
    - This can lead to policies that are defined too abstractly or for a particular domain in an imprecise manner.
- The integration of ontologies like the W3C Time Ontology can help overcome this limitation.
  - Adding new operators would allow more expressive policies.
- The extended ODRL could be applied in scenarios that require time-based privacy policies for IoT devices.
  - But this solution is only for a particular domain.

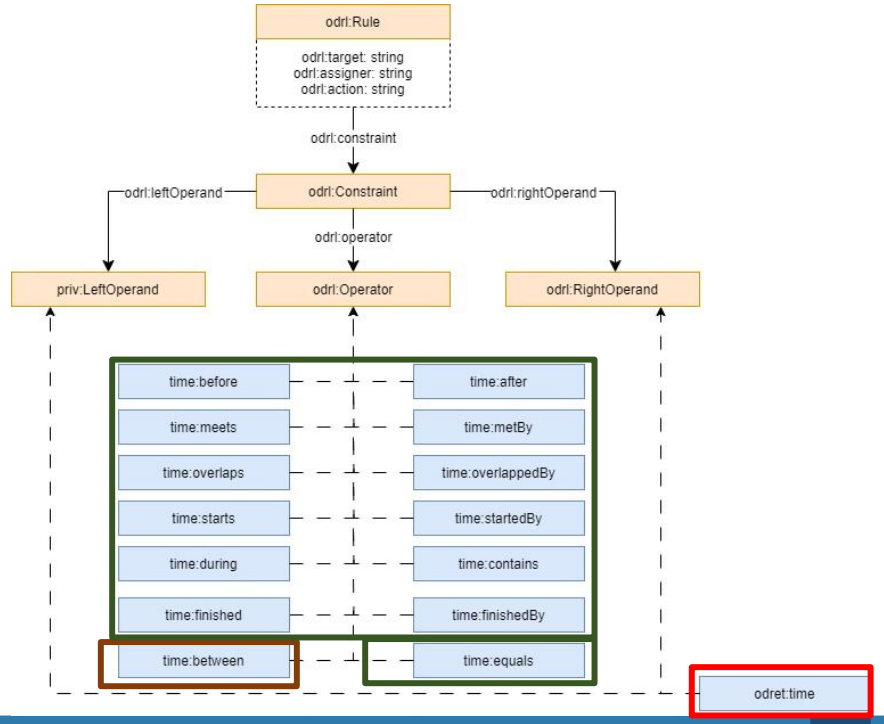
https://w3id.org/def/odre-time

Extending ODRL ontology. LOT methodology.




odrl:Rule
odrl:target: string
odrl:assigner: string
odrl:action: string
odrl:constraint
odrl:Constraint
odrl:leftOperand
odrl:rightOperand
odrl:operator
priv:LeftOperand
odrl:Operator
odrl:RightOperand
time:before
time:after
time:meets
time:metBy
time:overlaps
time:overlappedBy
time:starts
time:startedBy
time:during
time:contains
time:finished
time:finishedBy
time:between
time:equals
odret:time

- Time ontology. Added the time ontology classes (http://www.w3.org/2006/time#) to support time privacy policies.
- Between class (https://w3id.org/def/odre-time#between). Compares whether the date provided is between the times provided by right operand and left operand.
- Time class (https://w3id.org/def/odre-time#time). Class indicating that the system time is returned in operands.



Example of ODRL privacy policy with ODRL time

```
{
   "@context":["http://www.w3.org/ns/odrl.jsonld",
{"otime":"https://w3id.org/def/odre-time#"}
],
   "@type":"Offer",
   "uid":"http://example.com/policy:9090",
"permission":[
      {
         "target":"http://example.com/game:9090",
         "assigner":"http://example.com/org:xyz",
         "action":"play",
         "constraint":[
            {
               "leftOperand":{
                  "@value":"2017-12-31",
                  "@type":"xsd:date"
               },
               "operator":”otime:before",
               "rightOperand":{
                  "@value":"2019-12-31",
                  "@type":"xsd:date"
               }
            }
         ]
      }
   ]
}
```

```
{
   "@context":["http://www.w3.org/ns/odrl.jsonld",
      {"otime":"https://w3id.org/def/odre-time#"}
   ],
   "@type":"Policy",
   "uid":"https://upm.es/policy/19",
   "permission":[
      {
  "target":"https://jsonplaceholder.typicode.com/users/1",
         "action":"read",
         "constraint":[
            {
               "leftOperand":{
                  "@value":"06:55:00",
                  "@type":"xsd:date"
               },
               "operator":"otime:between",
               "rightOperand":{
                  "@value":"23:55:00",
                  "@type":"xsd:date"
               }
            }
         ]
      }
   ]
}
```

Conclusions

- ODRL recommendation has been widely adopted, but has certain limitations.
  - Ontological level, specification, expressiveness…
- This article aims to overcome the ontological level limitation defining how to extends ODRL.
  - With this time extension, domain-specific privacy policies can be built.
- Future work will consist of extending the ODRL privacy policies to support space-time privacy policies.

Towards time privacy policies in ODRL

Juan Cano de Benito, Andrea Cimmino, Raúl García-Castro
Ontology Engineering Group
Universidad Politécnica de Madrid
Spain

juan.cano@upm.e @jucanbe 17/09/2024 Amsterdam