AGAST authorisation: de-, de-, decentralise

Norman Gray
University of Leicester, UK

Baltimore Interop, 2008 October 29

agast project

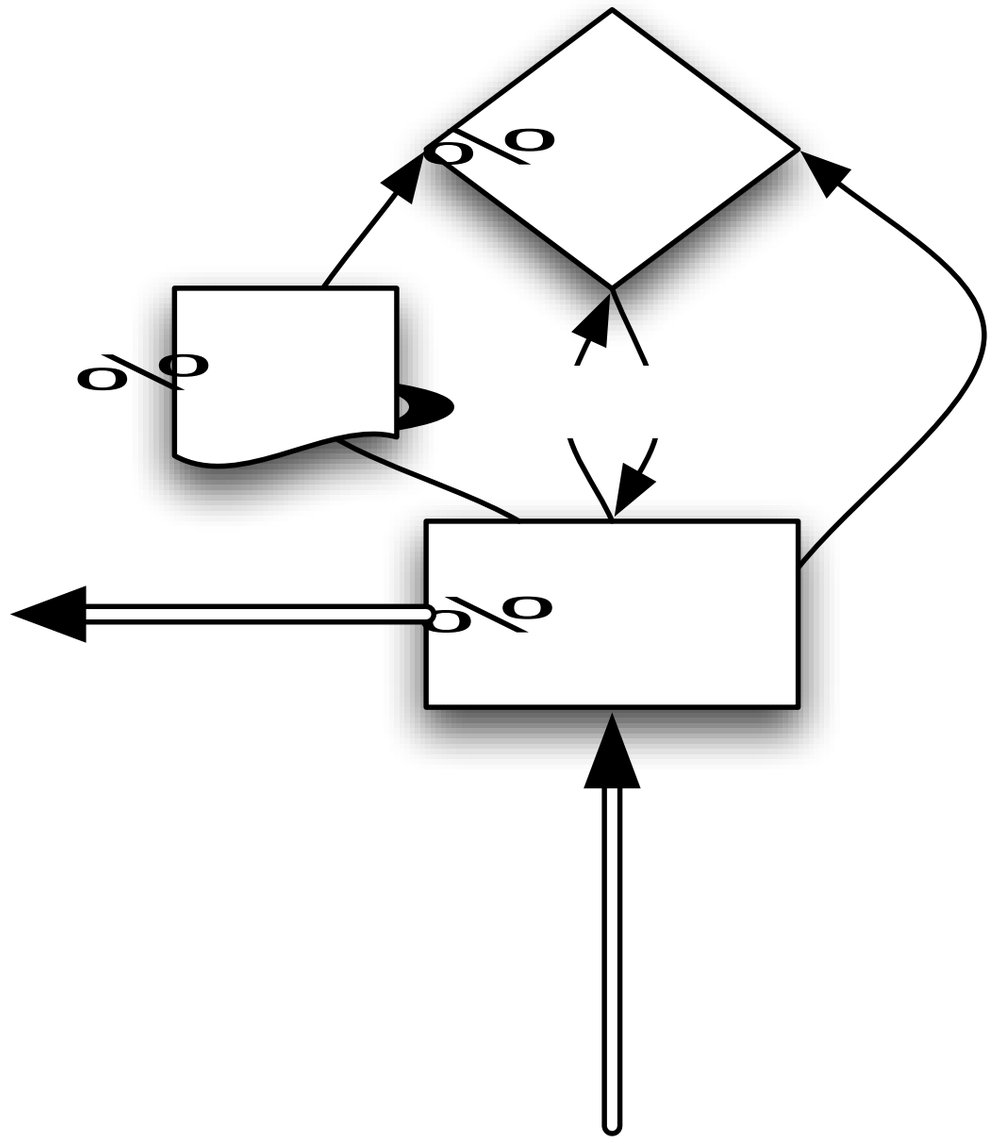
- JISC funded, to March 2009
- Norman Gray & Jeff Lusted, at Leicester; Richard Sinnott & Tom Doherty at NeSC Glasgow
- To produce use-cases (astronomy, bioinformatics, nanoelectronics and others), and prototype PDP implementation
- `http://www.nesc.ac.uk/hub/projects/agast/`

agast claim

- Advanced Grid Authorisation using Semantic Technologies
- There are multiple authorisation systems, of which PERMIS, Shibboleth and XACML are well-known
- But they're hard to use (lots of if-then-and-xor), hard to integrate, and don't do delegation/decentralisation naturally
- So take an alternative approach, based on class membership

agast

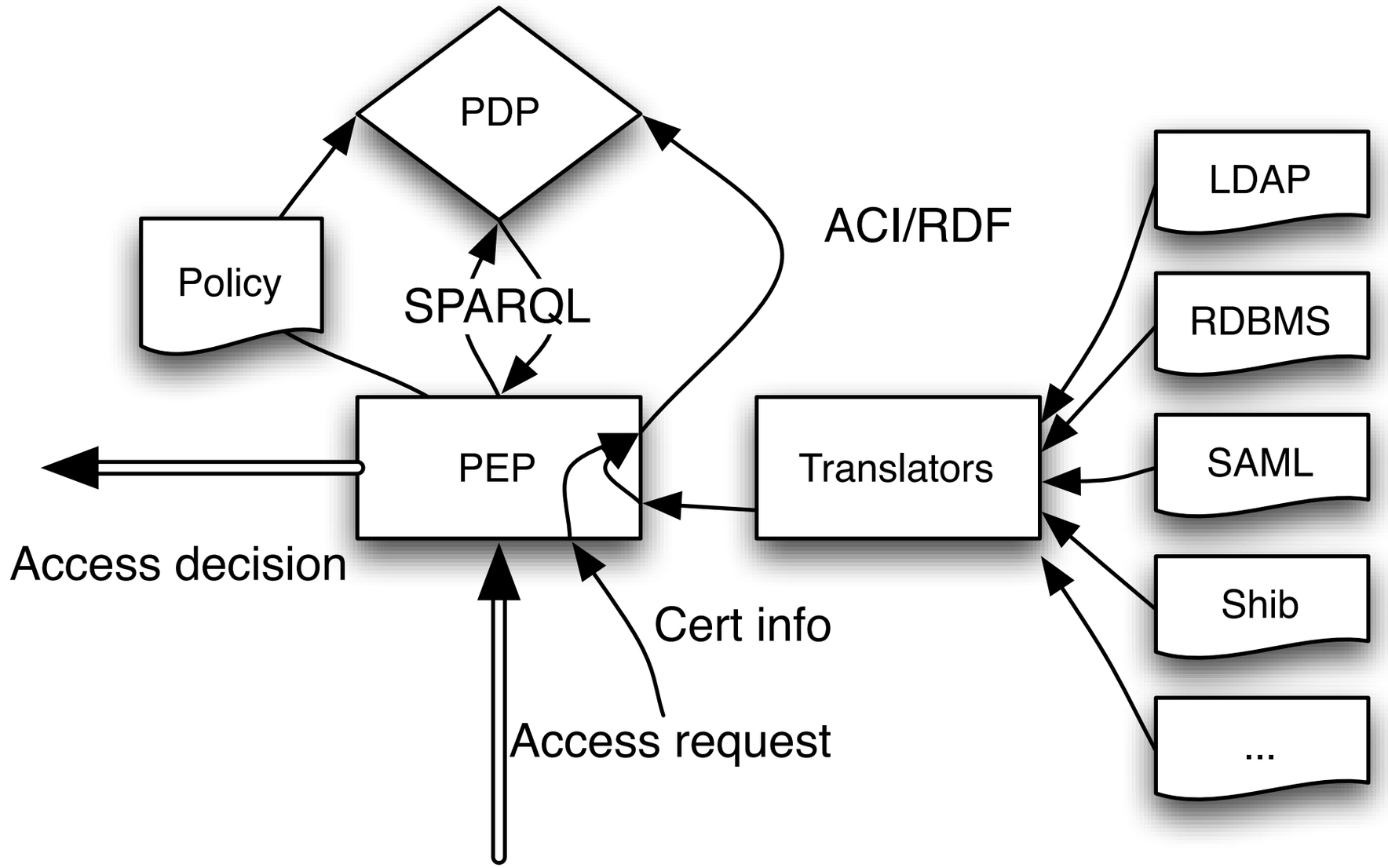
architecture



adf and adi

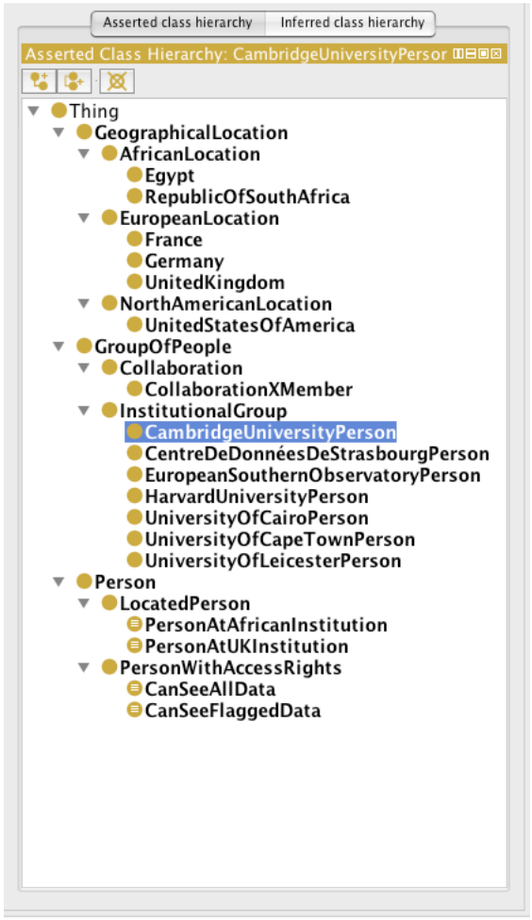
- PDP/ADF: Is user X provably a member of the class of people allowed to do Y?
- ADI: ontology defining relevant classes
- ADI: information about user X, expressed as RDF

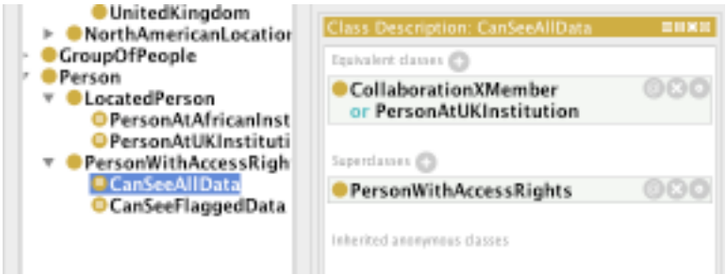
architecture with rdf



screenshot demo

- “Allow access from collaboration members, or members of european institutions; allow partial access to members of african institutions”
- An ontology of people and locations





Group and institution membership:

```
@prefix : <urn:example#> .
@prefix ac: <http://eurovotech.org/access-control.owl#> .

:Norman a ac:UniversityOfLeicesterPerson, ac:CollaborationXMember.
:Guy a ac:CambridgeUniversityPerson.
:Markus a ac:EuropeanSouthernObservatoryPerson.
:Sébastien a ac:CentreDeDonnéesDeStrasbourgPerson.
:Jonathan a ac:HarvardUniversityPerson;
        a ac:CollaborationXMember.
:Nelson a ac:UniversityOfCapeTownPerson;
        a ac:CollaborationXMember.
:Tutankhamun a ac:UniversityOfCairoPerson.
```

Equivalences:

```
@prefix owl: <http://www.w3.org/2002/07/owl#>.
<urn:example#Norman> owl:sameAs <mailto:norman@astro.gla.ac.uk>.
```

SPARQL:

```
prefix : <http://eurovotech.org/access-control.owl#>
ask { <mailto:norman@astro.gla.ac.uk> a :CanSeeAllData }
```

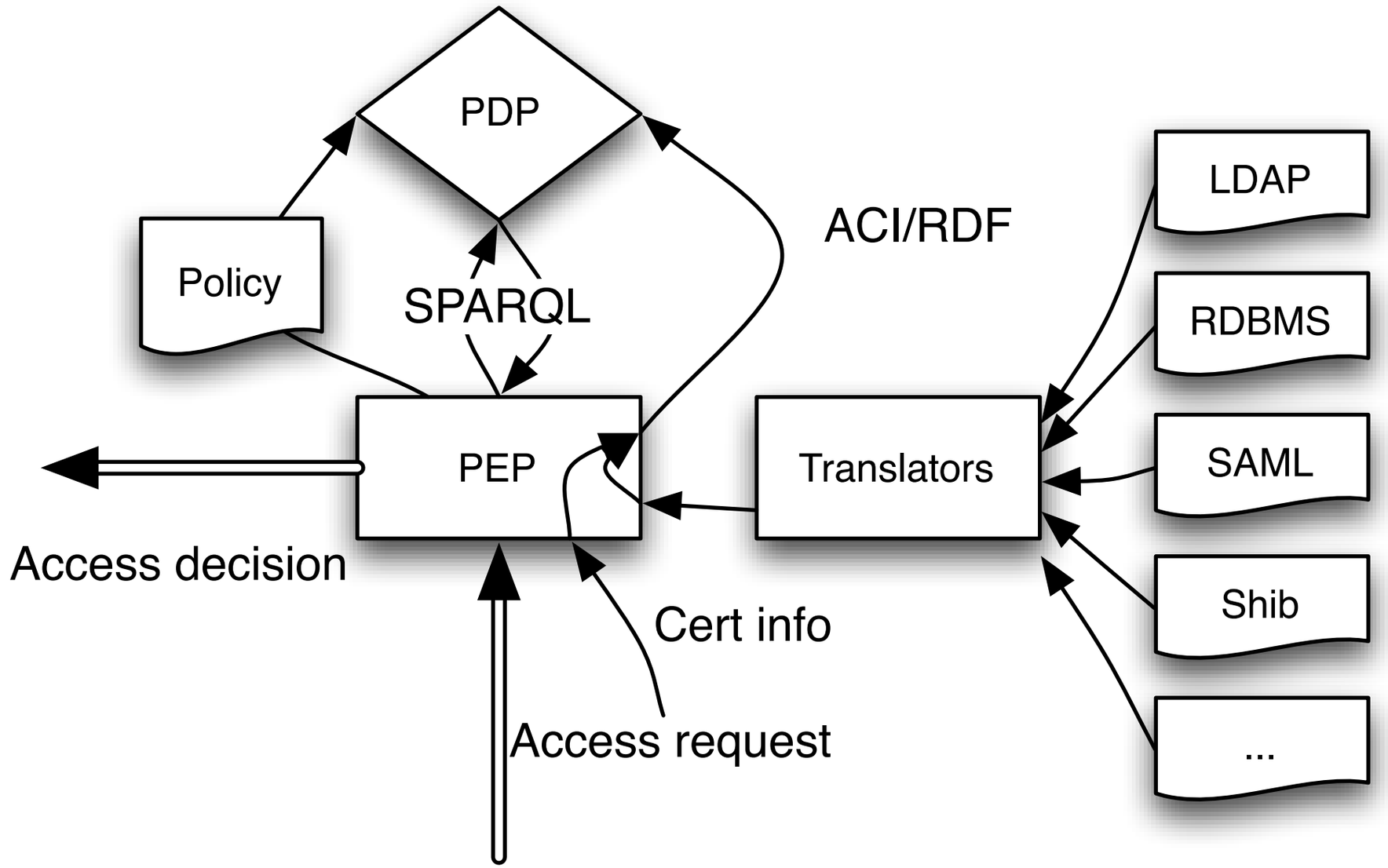
SPARQL:

```
prefix : <http://eurovotech.org/access-control.owl#>
select ?person
where { ?person a :CanSeeAllData }
```

using ‘curl’:

```
% curl --header content-type:application/sparql-query \
     --data-binary @access-all.rq \
     http://localhost:8080/quaestor/kb/testing \
    --header accept:text/csv
person
mailto:norman@astro.gla.ac.uk
urn:example#Norman
urn:example#Guy
urn:example#Nelson
urn:example#Jonathan
%
```

architecture with rdf



status

status

- identified relevant domains
- preliminary use-cases, due to be elaborated
- turning use-cases into ontological policies ... to come
- reasoner-based PDP prototyped

url

http://www.nesc.ac.uk/hub/projects/agast/

http://nxg.me.uk