Context-based authorizations for interactions in Hypermedia-Driven Agent Environments

The CASHMERE Framework

Alexandru SORICI, Adina Magda FLOREA

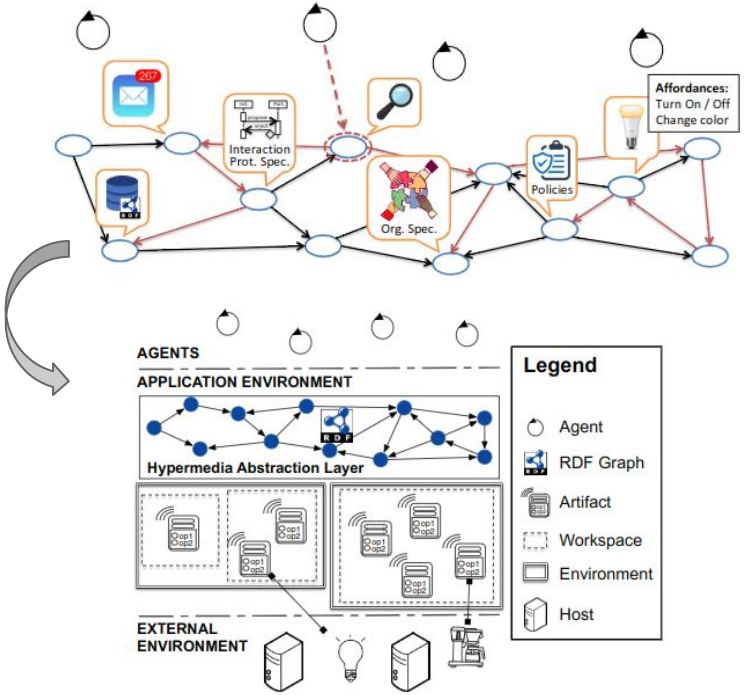
EMAS Workshop 2023

AI-MAS Group
"AIM AS high as you can"

The motivation and the opportunity

AI-MAS Group
"AIM AS high as you can"

Working Concepts and Principals

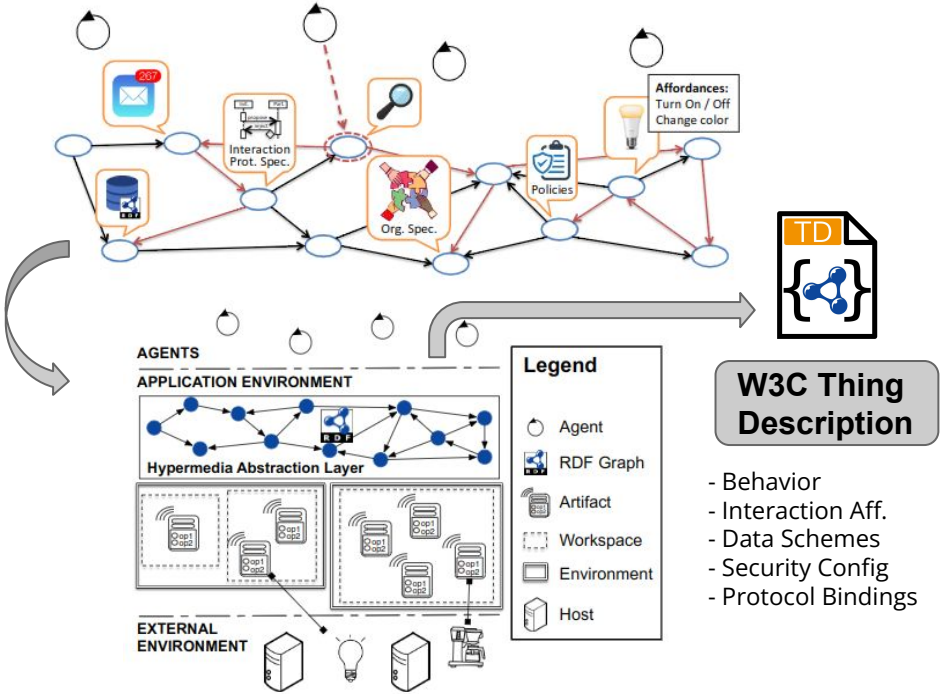


Hypermedia MAS

Ciortea et al, EMAS 2018
Ciortea et al, WoT 2019

AI-MAS Group
"AIM AS high as you can"

Working Concepts and Principals



W3C Thing Description

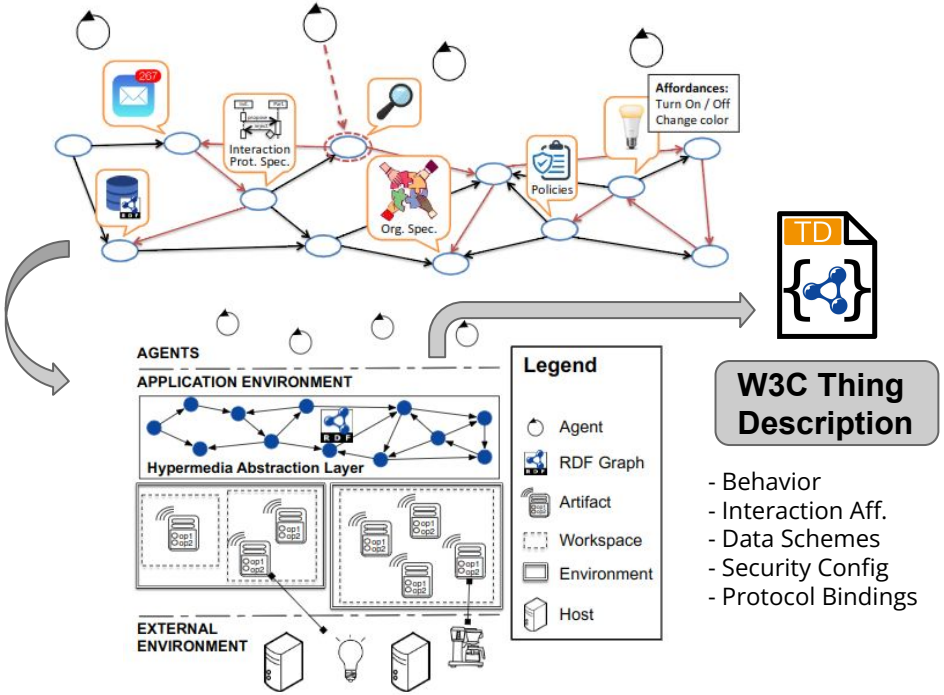
- Behavior
- Interaction Aff.
- Data Schemes
- Security Config
- Protocol Bindings

Hypermedia MAS

Ciortea et al, EMAS 2018
Ciortea et al, WoT 2019

AI-MAS Group
"AIM AS high as you can"

Working Concepts and Principals



W3C Thing Description

- Behavior
- Interaction Aff.
- Data Schemes
- Security Config
- Protocol Bindings

Hypermedia MAS

Ciortea et al, EMAS 2018
Ciortea et al, WoT 2019

Engineering of the Environment

- HATEOAS
- Uniform resource space
- Single Entry Point
- Observability

=> open, evolvable, long-lived, World-wide MAS

AI-MAS Group
"AIM AS high as you can"

Working Assumptions: Dynamic of Interactions

Hypermedia Artifacts include virtual and **real** Things

Hypermedia Agents are **mobile** in virtual and physical spaces

AI-MAS Group
"AIM AS high as you can"

Working Assumptions: Dynamic of Interactions

Hypermedia Artifacts include virtual and **real** Things

Hypermedia Agents are **mobile** in virtual and physical spaces

Agent dynamics, e.g.

- enter/exit an environment
- provide/remove a service/ resource/artifact
- Change roles
- Agent goals drive ***interest in*** Hypermedia resources

Ambient Intelligence (AmI) - principle of *locality*

- Interactions in AmI have ***situational boundaries***

AI-MAS Group
"AIM AS high as you can"

Working Assumptions: Dynamic of Interactions

Hypermedia Artifacts include virtual and **real** Things

Hypermedia Agents are **mobile** in virtual and physical spaces

Ambient Intelligence (AmI) - principle of *locality*

- Interactions in AmI have ***situational boundaries***

Agent dynamics, e.g.

- enter/exit an environment
- provide/remove a service/ resource/artifact
- Change roles
- Agent goals drive ***interest in*** Hypermedia resources

Environment Dynamics

- Hypermedia resources ***should*** be proactive to ***advertise*** changes in properties and affordances

AI-MAS Group
"AIM AS high as you can"

Working Assumptions: Dynamic of Interactions

Hypermedia Artifacts include virtual and **real** Things

Hypermedia Agents are **mobile** in virtual and physical spaces

Ambient Intelligence (AmI) - principle of *locality*

- Interactions in AmI have ***situational boundaries***

Agent dynamics, e.g.

- enter/exit an environment
- provide/remove a service/ resource/artifact
- Change roles
- Agent goals drive ***interest in*** Hypermedia resources

Environment Dynamics

- Hypermedia resources ***should*** be proactive to ***advertise*** changes in properties and affordances

Resources require a **mechanism** for managing **authorized interactions** while

"in context"

AI-MAS Group
"AIM AS high as you can"

Claims and Proposal

- Agent *mobility* + Observability Principle + AmI Locality Principle => **require *authorized interactions***
  - E.g. Simple running scenario: agent of person *employed as researcher* and *currently in lab* can interact with a smart light in the lab
- Dynamics of Agents + Environment **require** a ***dynamic access control mechanism***
  - Role-based access is not enough

AI-MAS Group
"AIM AS high as you can"

Claims and Proposal

- Agent *mobility* + Observability Principle + AmI Locality Principle => **require *authorized interactions***
  - E.g. Simple running scenario: agent of person *employed as researcher* and *currently in lab* can interact with a smart light in the lab
- Dynamics of Agents + Environment **require** a ***dynamic access control mechanism***
  - Role-based access is not enough

Proposal

- Hypermedia Artifacts ***should use*** an external **context-driven *Authorization Service***

AI-MAS Group
"AIM AS high as you can"

Context, Context Domains and Context-Based Authorization

AI-MAS Group
"AIM AS high as you can"

Context and Context Domains

Context

> "*Any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves*" [Dey, Understanding and using context, 2001]

Context info in a Hypermedia Environment:

- Properties and Affordances **of the** Hypermedia Artifacts
- Information **about the** Hypermedia Artifacts
- Information **about the** Agents

AI-MAS Group
"AIM AS high as you can"

Context and Context Domains

Context Dimensions and **Context Domains**[1]

- Means to ***organize*** context information

[1] Sorici et al, Multi-agent based flexible deployment of context management in ambient intelligence applications, 2015

Context and Context Domains

Context Dimensions and **Context Domains**[1]

- Means to ***organize*** context information

Context Dimensions: ***perspectives*** of logical partition of information (e.g. based on location, based on activity, based on organizational relations)

[1] Sorici et al, Multi-agent based flexible deployment of context management in ambient intelligence applications, 2015

AI-MAS Group
"AIM AS high as you can"

Context and Context Domains

Context Dimensions and **Context Domains**[1]

- Means to ***organize*** context information

Context Dimensions: ***perspectives*** of logical partition of information (e.g. based on location, based on activity, based on organizational relations)

Context Domains: ***view instances*** of **one or more** ***perspectives*** (e.g. Lab 308, Factory A, Assembly Process B, Teaching Activity C, membership relation D, ***employed users in Lab308***)

[1] Sorici et al, Multi-agent based flexible deployment of context management in ambient intelligence applications, 2015

AI-MAS Group
"AIM AS high as you can"

Shared Context

AmI Principle [Olaru et al, 2013]: entities that *share context* **should** exchange information / interact

Context Domains model logical partitions of context information *from one or more perspectives* (the Context Dimensions): e.g. all information *from* and *about owned* Things and *employed* Agents in Lab 308

[Olaru et al, 2013] A context-aware multi-agent system as a middleware for ambient intelligence, Mobile Networks and Applications, No. 18

AI-MAS Group
"AIM AS high as you can"

Shared Context

AmI Principle [Olaru et al, 2013]: entities that *share context* **should** exchange information / interact

Context Domains model logical partitions of context information *from one or more perspectives* (the Context Dimensions): e.g. all information *from* and *about owned* Things and *employed* Agents in Lab 308

Two entities ***share context*** if a subset of context information *from* or *about them* is included in at least one Context Domain of the application.

[Olaru et al, 2013] A context-aware multi-agent system as a middleware for ambient intelligence, Mobile Networks and Applications, No. 18

AI-MAS Group
"AIM AS high as you can"

Shared Context

Simplified, ***organizational*** view

Context Domain ----------> Context Domain **Group**

Shared Context ----------> **Membership** in Context Domain Group

AI-MAS Group
"AIM AS high as you can"

Shared Context

Simplified, ***organizational*** view

Context Domain ----------> Context Domain **Group**

Shared Context ----------> **Membership** in Context Domain Group

Shared Context Identification

- Rule-based reasoning that describes **the conditions** that **count towards membership** in a Context Domain

AI-MAS Group
"AIM AS high as you can"

Engineering Shared Context Identification

RDF Stream Reasoning: "*define common models for producing, transmitting and continuously querying RDF Streams*"[1] (e.g. C-SPARQL[2])

SOLID Web Access Control[3]:

- Workhorse structure: ACL policy - specify access control policies
- Grant authorization of *Read*, *Write/Update*, *Control*
- Authorization granted *by agent, by agent class (e.g. foaf:Person), by* ***group membership***

[1] https://streamreasoning.org/

[2] Barbieri et al, C-sparql: a continuous query language for rdf data streams, 2010

[3] https://solid.github.io/web-access-control-spec/

```
PREFIX consert: <http://pervasive.semanticweb.org/ont/2017/07/consert/core/>
PREFIX ann: <http://pervasive.semanticweb.org/ont/2017/07/consert/annotation/>
PREFIX foaf: <http://xmlns.com/foaf/0.1/>
PREFIX vcard: <http://www.w3.org/2006/vcard/ns#>
PREFIX precis: <http://aimas.cs.pub.ro/consert/ontologies/precis#>

REGISTER STREAM <SharedLab308Context> AS
CONSTRUCT ISTREAM {
    precis:lab308group vcard:member ?agent .
}
FROM NAMED :staticAssertions
FROM NAMED :profiledAssertions
FROM NAMED WINDOW :pLoc [RANGE PT10S STEP PT10S] ON STREAM :PersonLocated
WHERE
{
    GRAPH :staticAssertions { ?agent rdf:type foaf:Person . }
    GRAPH :profiledAssertions {
        ?worksAssertion a precis:WorksAt ;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:upb ;
            ann:hasAnnotation ?validAnn .
        ?validAnn a ann:TemporalValidityAnnotation ;
            ann:startTime ?employmentStart ;
            ann:endTime ?employmentEnd .
    }
    WINDOW :pLoc {
        ?persLocAssertion a precis:LocatedAt;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:lab308 .
    }
    BIND (xsd:dateTime(NOW()) AS ?date)
    FILTER (?date > ?employmentStart && ?date < ?employmentEnd)
}
```

Output of reasoning: **stream** of **Context Domain group memberships**

Engineering Context Based Authorization

AI-MAS Group
"AIM AS high as you can"

```
PREFIX consert: <http://pervasive.semanticweb.org/ont/2017/07/consert/core/>
PREFIX ann: <http://pervasive.semanticweb.org/ont/2017/07/consert/annotation/>
PREFIX foaf: <http://xmlns.com/foaf/0.1/>
PREFIX vcard: <http://www.w3.org/2006/vcard/ns#>
PREFIX precis: <http://aimas.cs.pub.ro/consert/ontologies/precis#>

REGISTER STREAM <SharedLab308Context> AS
CONSTRUCT ISTREAM {
    precis:lab308group vcard:member ?agent .
}
FROM NAMED :staticAssertions
FROM NAMED :profiledAssertions
FROM NAMED WINDOW :pLoc [RANGE PT10S STEP PT10S] ON STREAM :PersonLocated
WHERE
{
    GRAPH :staticAssertions { ?agent rdf:type foaf:Person . }
    GRAPH :profiledAssertions {
        ?worksAssertion a precis:WorksAt ;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:upb ;
            ann:hasAnnotation ?validAnn .
        ?validAnn a ann:TemporalValidityAnnotation ;
            ann:startTime ?employmentStart ;
            ann:endTime ?employmentEnd .
    }
    WINDOW :pLoc {
        ?persLocAssertion a precis:LocatedAt;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:lab308 .
    }
    BIND (xsd:dateTime(NOW()) AS ?date)
    FILTER (?date > ?employmentStart && ?date < ?employmentEnd)
}
```

Output of reasoning: **stream** of **Context Domain group memberships**

Reasoning over ***snapshot windows*** of dynamic information (agent location)

Engineering Context Based Authorization

AI-MAS Group
"AIM AS high as you can"

```
PREFIX consert: <http://pervasive.semanticweb.org/ont/2017/07/consert/core/>
PREFIX ann: <http://pervasive.semanticweb.org/ont/2017/07/consert/annotation/>
PREFIX foaf: <http://xmlns.com/foaf/0.1/>
PREFIX vcard: <http://www.w3.org/2006/vcard/ns#>
PREFIX precis: <http://aimas.cs.pub.ro/consert/ontologies/precis#>

REGISTER STREAM <SharedLab308Context> AS
CONSTRUCT ISTREAM {
    precis:lab308group vcard:member ?agent .
}
FROM NAMED :staticAssertions
FROM NAMED :profiledAssertions
FROM NAMED WINDOW :pLoc [RANGE PT10S STEP PT10S] ON STREAM :PersonLocated
WHERE
{
    GRAPH :staticAssertions { ?agent rdf:type foaf:Person . }
    GRAPH :profiledAssertions {
        ?worksAssertion a precis:WorksAt ;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:upb ;
            ann:hasAnnotation ?validAnn .
        ?validAnn a ann:TemporalValidityAnnotation ;
            ann:startTime ?employmentStart ;
            ann:endTime ?employmentEnd .
    }
    WINDOW :pLoc {
        ?persLocAssertion a precis:LocatedAt;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:lab308 .
    }
    BIND (xsd:dateTime(NOW()) AS ?date)
    FILTER (?date > ?employmentStart && ?date < ?employmentEnd)
}
```

Output of reasoning: **stream** of **Context Domain group memberships**

Reasoning over ***snapshot windows*** of dynamic information (agent location)

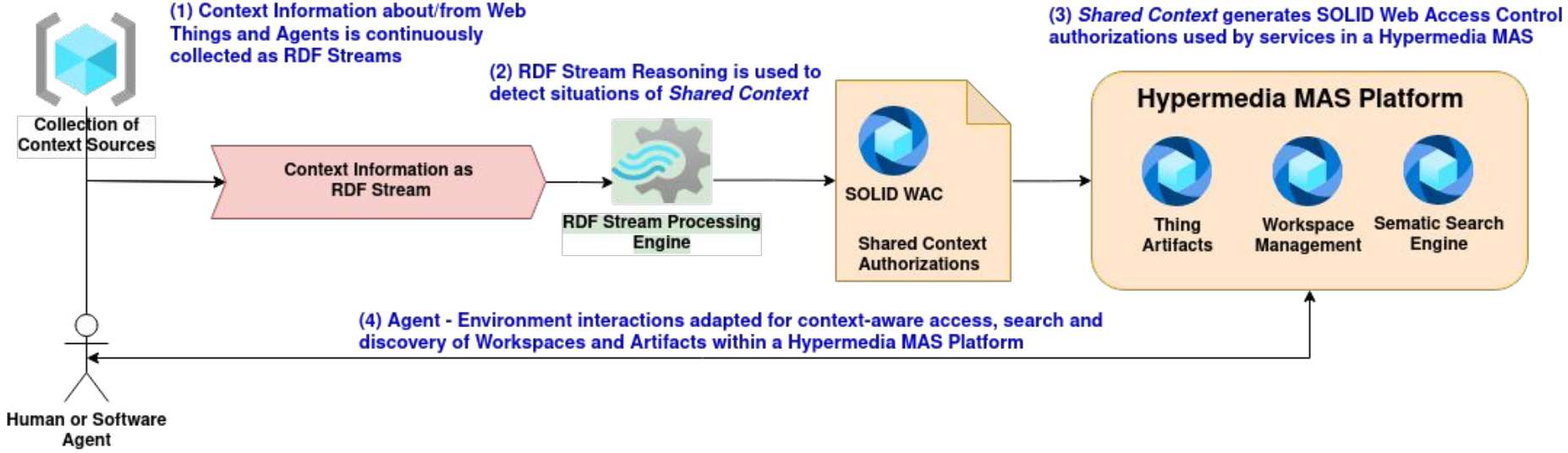
Conditions combine *static, profiled* and *dynamic/sensed* context information

Engineering Context Based Authorization

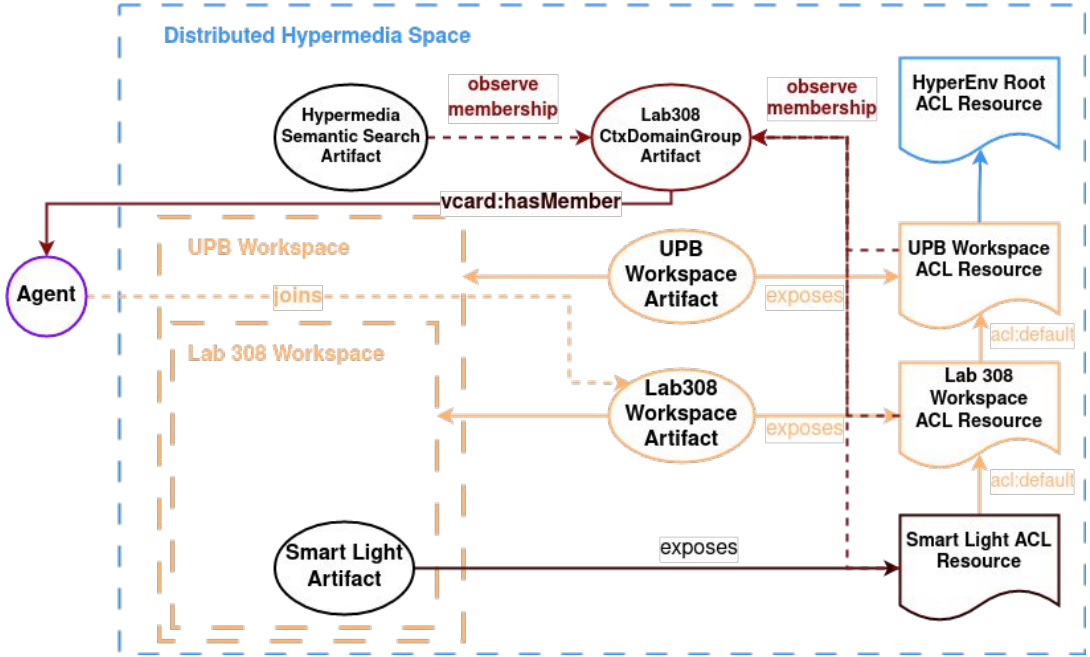
CASHMERE and Hypermedia Envs - Integration

AI-MAS Group
"AIM AS high as you can"

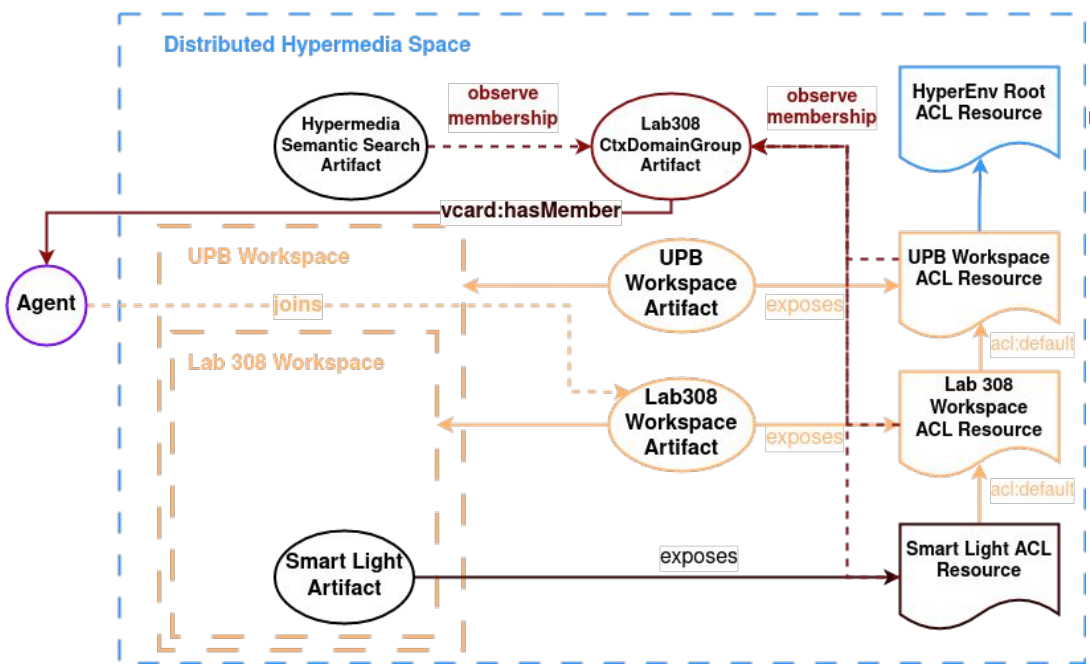
Integration High level View



Integration in a Hypermedia MAS



Integration in a Hypermedia MAS




```
[ ] a acl:Authorization;
    acl:accessTo ex:UPBWspAcl,
       ex:Lab308WspACL, ex:SmartLightACL;
    acl:mode acl:Control;
    acl:agent ex:HyperEnvOwner.
```

```
[ ] a acl:Authorization;
    acl:accessTo ex:Lab308Wsp;
    acl:default ex:UPBWsp;
    acl:mode acl:Write;
    acl:agentClass foaf:Person.
```

```
[ ] a acl:Authorization;
    acl:accessTo ex:SmartLight;
    acl:default ex:Lab308Wsp;
    acl:mode acl:Read, acl:Write;
    acl:agentGroup ex:Lab308CtxDomain.
```

AI-MAS Group
"AIM AS high as you can"

Integration Roadmap

- Develop PoC Engine that performs ***shared context identification*** **DONE**

- Integration with Yggdrasil[1] **In progress**
  - Modify HypermediaArtifact init() to specify *observed* Context Domain groups
  - A WAC Service is created to handle
    - Retrieval WAC Resource repr. for Artifact / Wsp / Env
    - Add / remove WAC Authorizations (using SPARQL statements)
    - **Validate Authorizations** → **validation Engine** requires SPARQL Federated queries to check group **memberships** of one or more Context Domain Group Artifacts

[1] Ciortea et al, Engineering world-wide multi-agent systems with hypermedia, EMAS 2018

Takeaways and Thank You!

- Agent and Env. dynamics of Hypermedia Envs **warrant *context-based authorized access*** to hypermedia resources
- Context information *of* and *about* hypermedia resources is organized into **Context Domains**
- Shared Context is modeled as **membership in** a ***Context Domain Group***
- **Shared Context Identification** uses **RDF Stream Reasoning** technologies to output **SOLID Web Access Control Authorizations**
- **Yggdrasil + CASHMERE** integration roadmap planned

THANK YOU!

AI-MAS Group
"AIM AS high as you can"