Policy Transformation within The Eclipse Dataspace Connector (EDC)

Overview and Results

Amjad Ibrahim*, Antonio La Marra, *Alessandro Rosetti**,

Theo Dimitrakos

German Research Center, *Huawei Technologies, Munich*

Security Forge, Pisa

*amjad.Ibrahim@huawei.com

Who are we?

Research team in Huawei Munich Research Center

Trustworthy Technology and Engineering Laboratory

R&D team from Security Forge

A spin-off startup of CNR Italy

Interested in:

Dynamic authorization

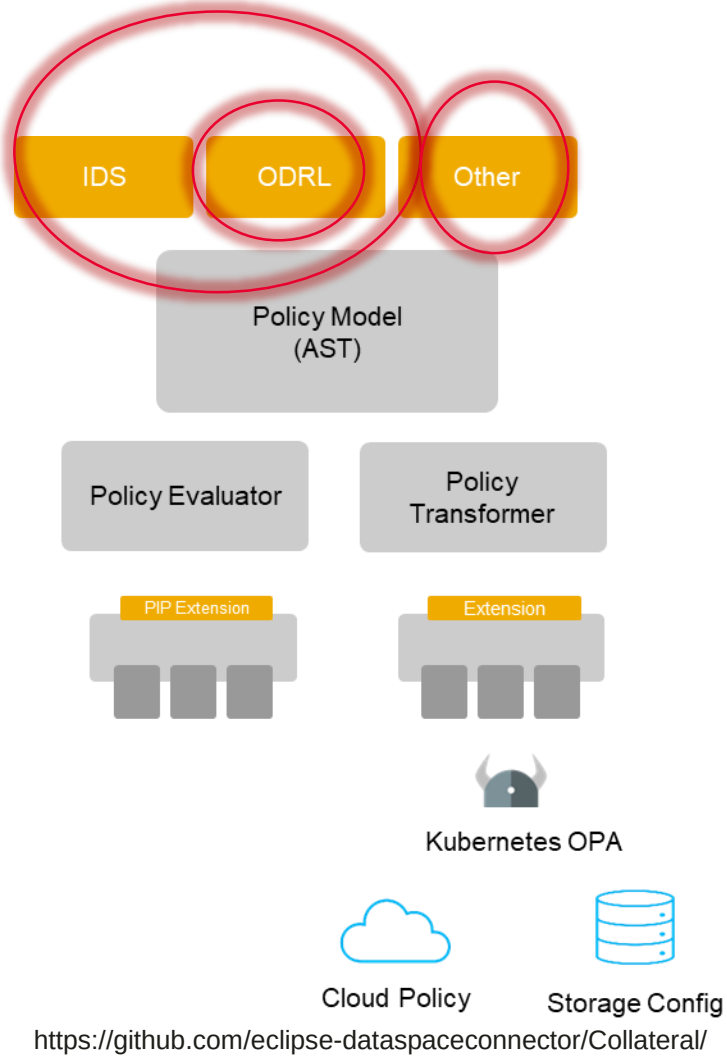
Identity and Access management systems

Privacy-enhancing technologies

Usage Control

EDC Policy Design

- EDC uses ODRL to express policies
  - ODRL and ABAC (XACMLv3) have been around for a while and the issue of how they relate to each other is important
  - ODRL models digital rights without a reference architecture and XACML is a security access/usage standard
- EDC Uses IDS/ODRL as declarative high-level language about rights and contracts and is open for extension
- How about interoperability, relation, refinement with other languages and standards?



https://github.com/eclipse-dataspaceconnector/Collateral/

HUAWEI

Background: Open Digital Rights Language (ODRL)*

- A rights with **vocabulary** for representing statements concerning the **rights** regarding **digital resources**
- A *Policy* contains ***Permissions*** and ***Prohibitions, Duties***
  - act on ***Action***, executed over an ***Asset*** by a ***Party***
  - can be limited by ***Constraints***
  - Constraints have a *name* (e.g. count), an *operator* (e.g. leq), a *right operand* (e.g. '5') and possibly an *status (e.g. '3')* "*The action may be exercised 5 times, and currently it has already been executed 3"*
- Provides with common vocabulary
  - 60 actions, to be used in permissions, prohibitions and duties: **copy**, **delete**, **modify**, **inform**
  - 30 constraints: **language**, **count**, **dateTime**, **industry**
  - 12 operators: **eq**, **gt**, **isPartOf**
  - 7 kinds of roles: **assigner**, **assignee**…
  - 6 scopes for the roles: **individual**, **all**, **group**,

*Based on: Víctor Rodríguez-Doncel, ODRL2.0: A Rights Expression Language and a Policy Language *Tutorial.*

Reflections on ODRL*

- High coupling of business and authorization logic in the enforcement engine
  - > E.g., an enum of 17 supported constraint in the IDS connector (see https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/873)
  - > Constraints e.g., count, location are fixed in the standard
- Few (found only one) open-source evaluators
- Aspects of delegation, e.g. the revocation of rights, granting redistribution rights cannot be fully specified
  - > Expressions in ODRL provide terms for specifying expiration dates (constraint class) but do not consider updating activities
- Handling conflicts: ODRL provides a strategy to resolve conflicts that arise when merging policies due to policy inheritance. It uses the conflict property which can take either the **perm**, **prohibit** only
- Not all ODRL terms are part of the IDS Usage Control language as the requirements slightly differ
  - > "… the IDS Usage Control Language was initially defined as a **profile** of ODRL Language. So we could extend the ODRL concepts. Later on, IDS language grew even more and now they match in many cases, however, they have few differences."
    - https://github.com/International-Data-Spaces-Association/InformationModel/issues/523
    - https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/873

*More on limitations in: Milen G. KEBEDE et al., ODRL2.0: A critical reflection on ODRL. *https://enablingpersonalizedinterventions.nl/2020-12-09/AICOL2020.pdf*

Page 5

Scope, Goal, and Plan

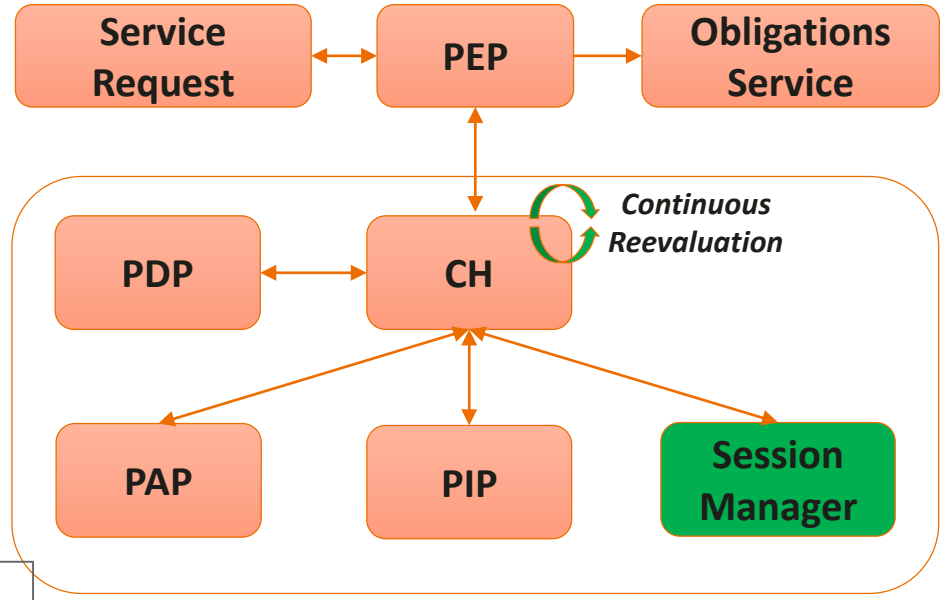
- Different sets of supported policy models
- Hard to design a comprehensive ODRL-ALFA transformation that is compliant with the adapted versions
  - > As a first step we will build a component that accepts ODRL policies, and do a translation based on a simplistic mapping to show how EDC-UCON can interface other languages

- A better integration of UCON within the EDC
  - > UCON understands native EDC policies
  - > Deal with some of the limitations
  - > Identify the relations and capabilities of the two languages

- Understand the mapping between the ODRL and XACML models
- Implement a PoC that outputs ALFA policies based on ODRL policies
- Demonstrate this with our EDC-UCON integration results from last hackathon

Background: Usage Control System: UCON Model

- The goal of Usage Control is to make sure that specified usage restrictions and obligations are realized even after access to data has been granted
- The Usage Control System implements the ABAC authorization model based on the eXtensible Access Control Markup Language (XACML) standard
  - Support usage control through continuous authorization
  - ALFA (profile) is less verbose and more compact than XACML
  - Faster parsing and evaluation

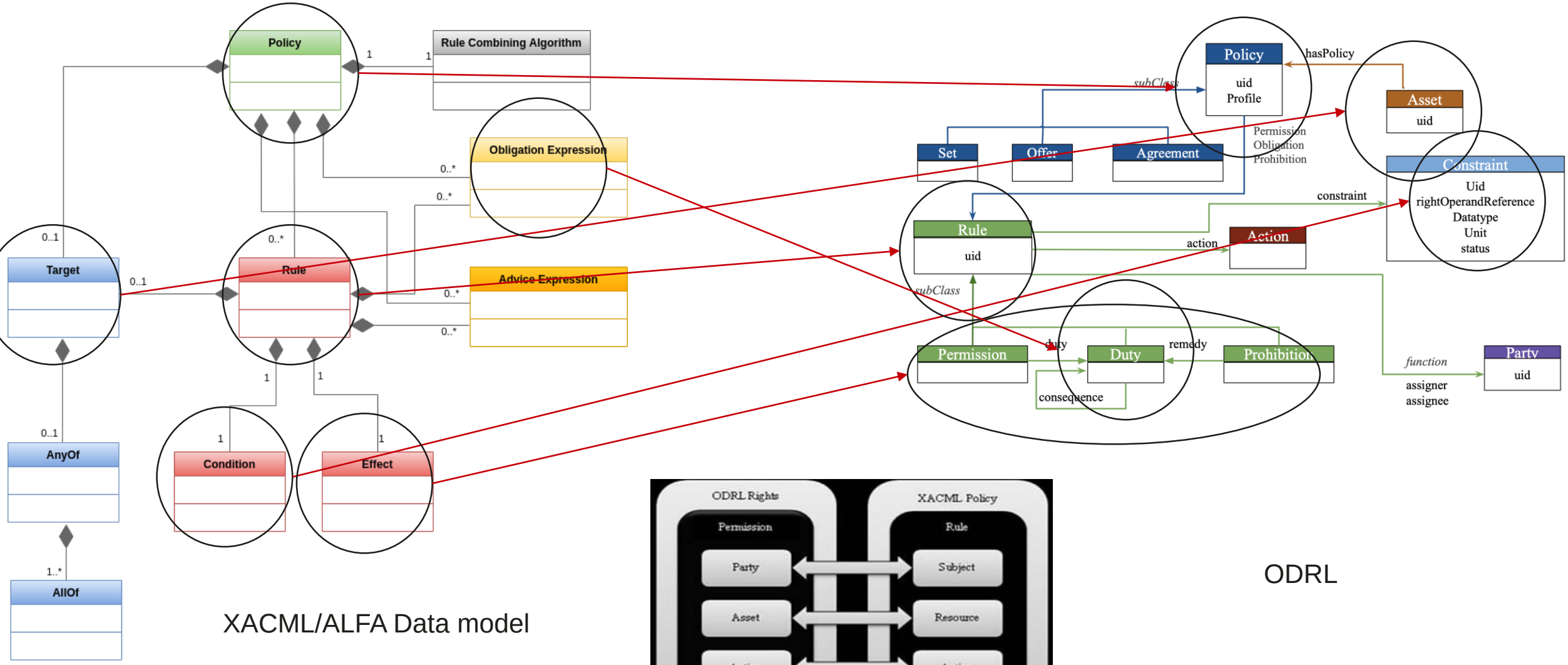


Commercial:
NTT / Axiomatics Federal
Axiomatics (Nordea, PayPal, BoA, Bell H, …)
Next Labs (SAP, BAE Systems, Siemens, Microsoft, …)
Oracle, Atos, Ping. Empower ID,, PlainID, Symphonic, WSO2

Open source:
Balana, AuthZForce, FIWARE IDM, …

HUAWEI

The mapping



XACML/ALFA Data model

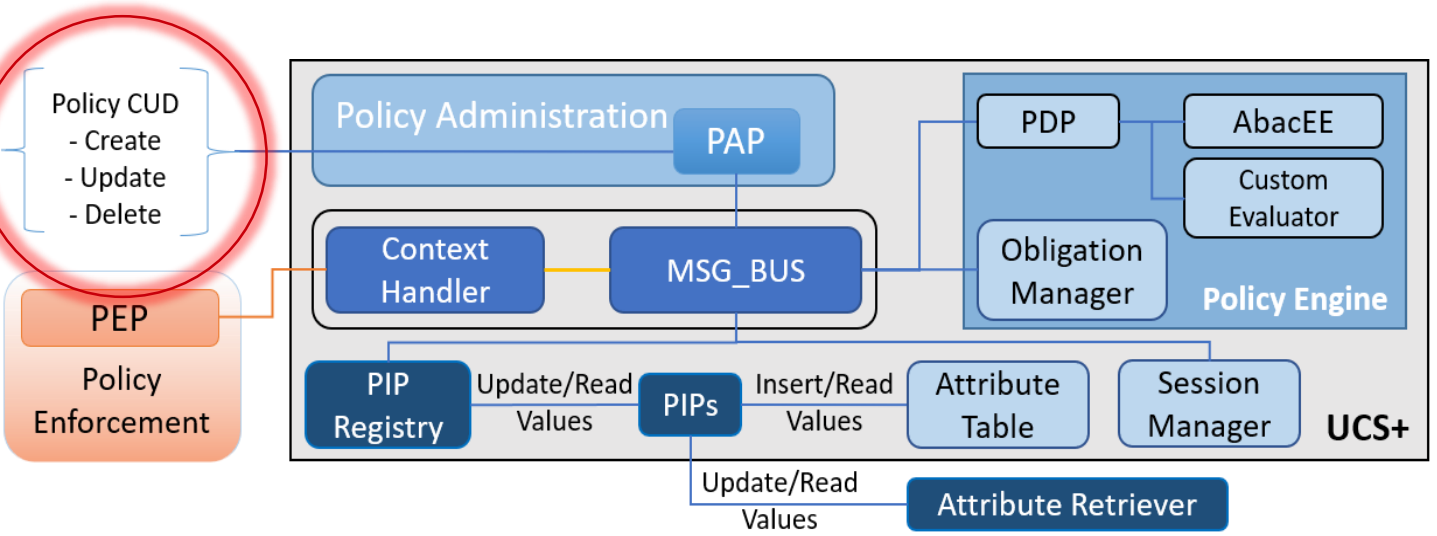
ODRL

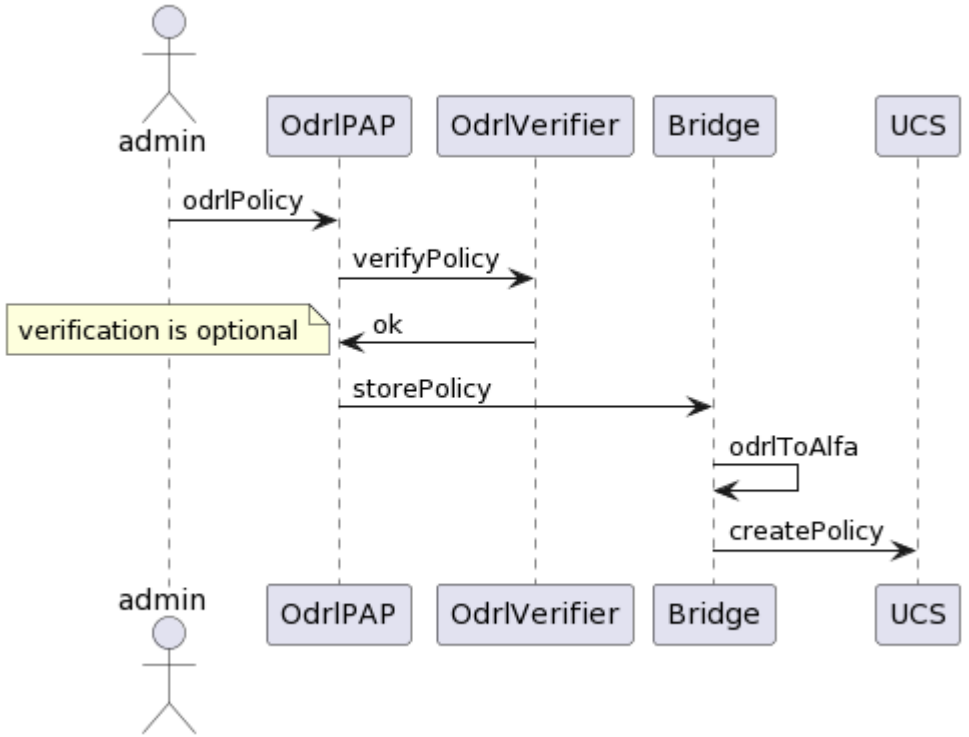
https://medium.com/identity-beyond-borders/a-beginners-guide-to-xacml-6dc75b547d55

HUAWEI

Usage Control System Plus (UCON+)

- Incorporates an ABAC baseline and extends it with:
  - **Policy-based** and **codeless** behaviour
  - **Continuous monitoring** of context and resource access





- PAP: policy administration point that receives ODRL

HUAWEI

Hackathon#2 → 3: Bringing Usage Control (UCON+) into EDC

✓EDC-UCS extension

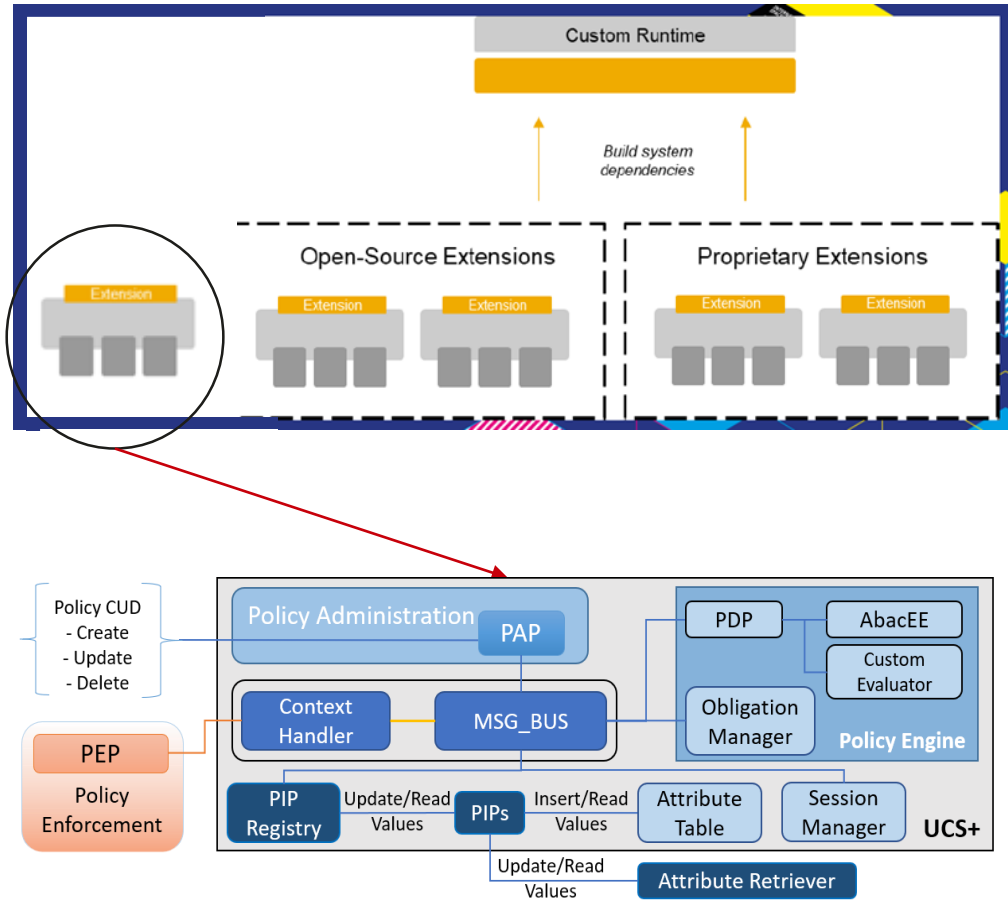
- ✓ EDC has an access control mechanism that directly evaluates ODRL policies. We extended it with UCON+ to enforce ALFA

- Now, we **added** an interface that gets ODRL and then transform it to ALFA

✓Custom Policy Enforcement Points (PEP) and privacy-preserving obligation for 1 EDC samples

- ✓ File transfer

- Achieved the goal of capturing the commonality between ODRL and ALFA which allows for interoperability and better integration of existing systems, **BUT**
  - > in a limited scope, and with a simplistic mapping
  - > this can be achieved with more comprehensive approaches, e.g., using template, using an editor



HUAWEI

Demo: step1 ODRL to ALFA converter

- Analyze ODRL policy
- Convert permission / prohibition, constraints and obligations into ALFA

```
{
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "Offer",
    "uid": "anon",
    "profile": "http://example.com/odrl:profile:01",
    "permission": [{
        "uid" : "anonymize",
        "obligation" : [{
                "uid" : "http",
                "url" : "http://localhost:8181/api/anonymize",
                "method" : "POST",
                "body" : "{\\\"type\\\" : \\\"partial-user-email-anonymize\\\"
, \\\"source\\\" : \\\"\\\", \\\"destination\\\" : \\\"\\\"}",
                "headers" : "Content-Type:application/json"
        }]
    }]
}
```

```
policy anon {
        apply denyOverrides
        rule anonymize {
                permit

                on permit {
                        obligation http {
                                url = 'http://localhost:8181/api/anonymize'
                                body = '{\"type\" : \"partial-user-email-anony
mize\", \"source\" : \"\", \"destination\" : \"\"}'
                                headers = 'Content-Type:application/json'
                                method = 'POST'
                        }
                }
        }
}
```

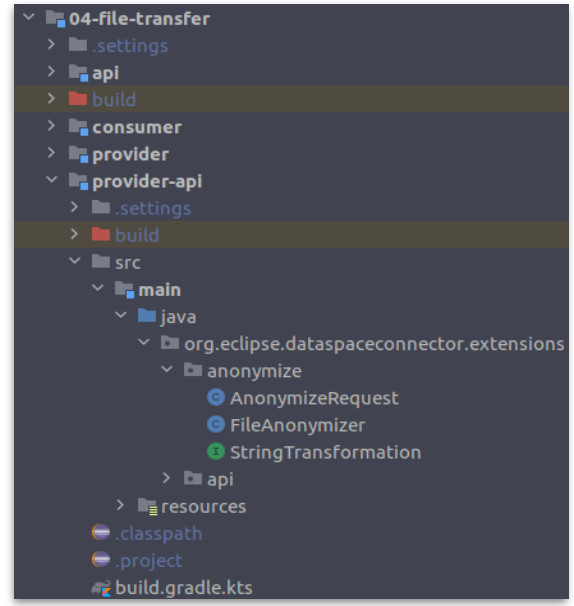
HUAWEI

Demo: step2 Anonymizing emails in File Transfer sample

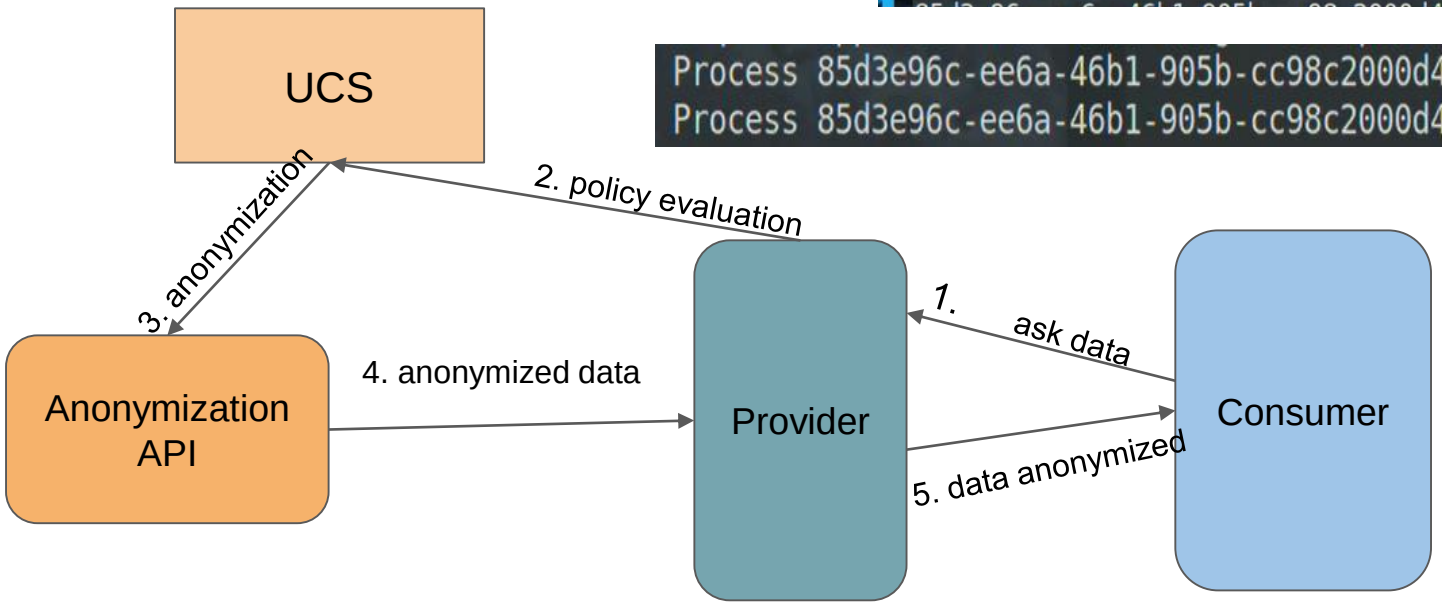
- The file contents will be anonymized by anonymizing any email text with a regex
  alice@company.it -> ali***@***

```
{
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "Offer",
    "uid": "anon",
    "profile": "http://example.com/odrl:profile:01",
    "permission": [{
        "uid" : "anonymize",
        "obligation" : [{
                "uid" : "http",
                "url" : "http://localhost:8181/api/anonymize",
                "method" : "POST",
                "body" : "{\\\"type\\\" : \\\"partial-user-email-anonymize\\\"
, \\\"source\\\" : \\\"\\\", \\\"destination\\\" : \\\"\\\"}",
                "headers" : "Content-Type:application/json"
        }]
    }]
}
```

```
roarc at static in ~/workspace
./run-file-transfer-curl.sh
```




```
Process 85d3e96c-ee6a-46b1-905b-cc98c2000d42 is now IN_PROGRESS
Process 85d3e96c-ee6a-46b1-905b-cc98c2000d42 is now COMPLETED
```




```
acm***@acme.com
cia***@sec.com
hel***@hello.it
```

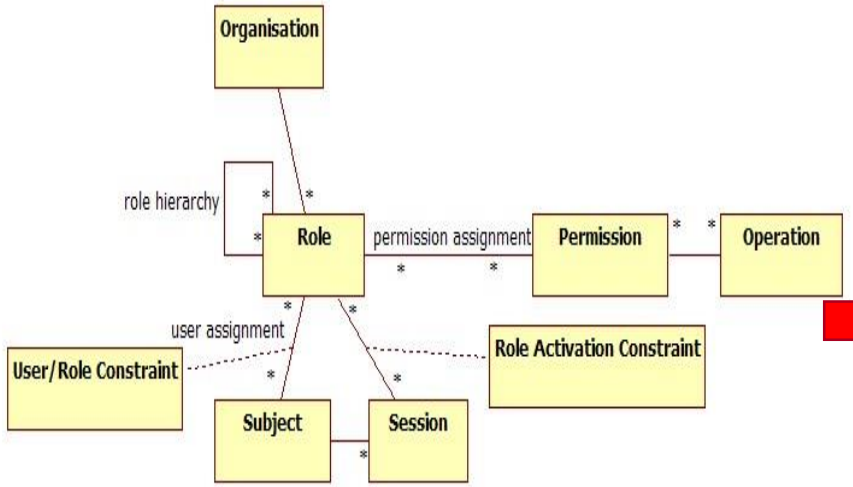
Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.

Back-up Content

Access management from Role Based to UCON

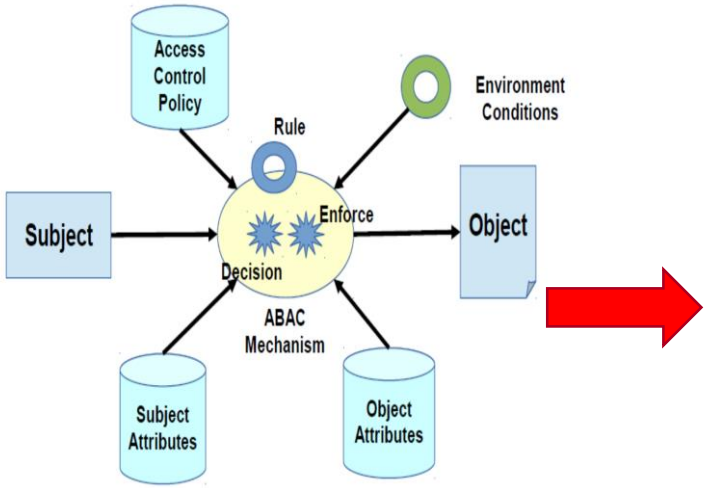
RBAC
Role Based Access Control



Access decisions are made based on:

- User role in organization
- Role permissions
- Role relationships

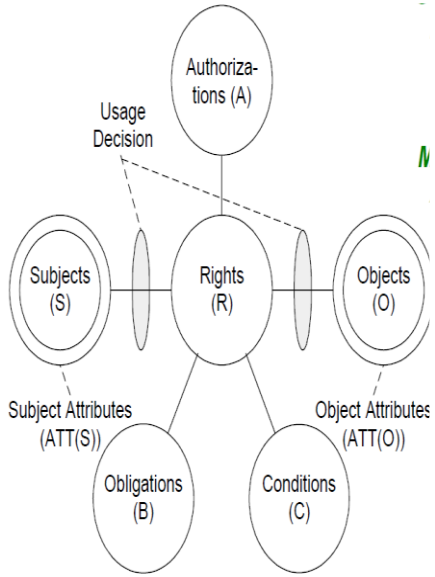
ABAC
Attribute Based Access Control



Access decisions are made based on:

- Subject attributes
- Object attributes
- Environment conditions

UCON
Usage Control ABAC



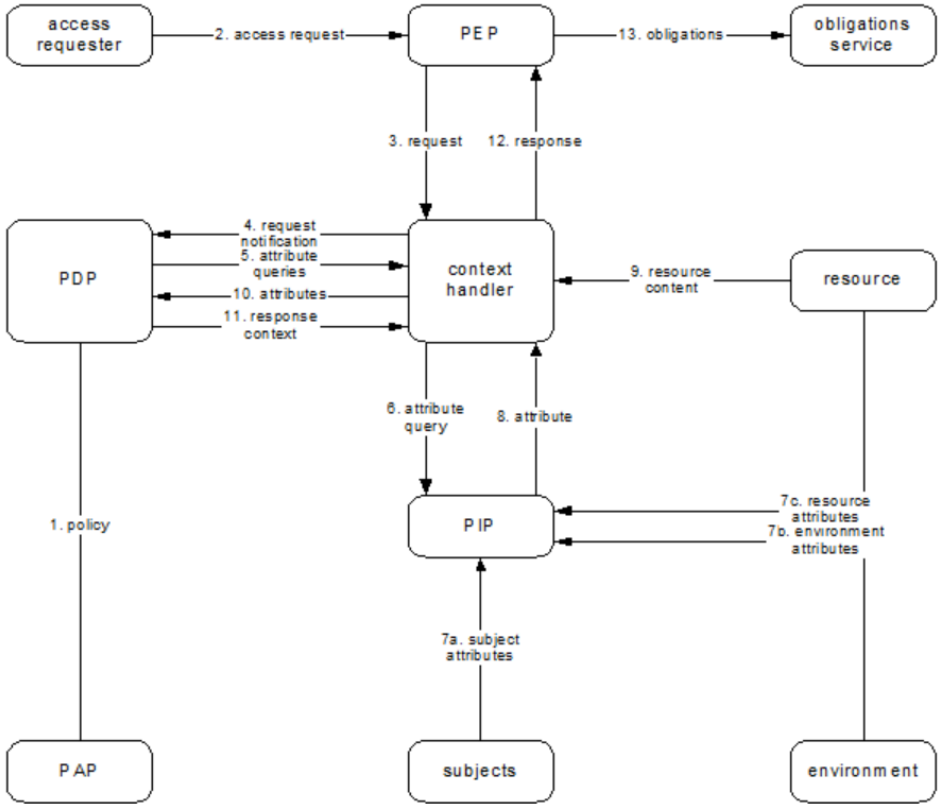
UCON is ABAC Plus:

- Continuity
  - Decisions can be made during usage for continuous enforcement
- Mutability
  - Attributes can be updated as side-effect of subject actions

The goal of Usage Control is to make sure that specified usage restrictions and obligations are realized even after access to data has been granted

HUAWEI

Background: ABAC



- **PAP** (Policy Administration Point): administer policies
- **PEP** (Policy Enforcement Point)
  - PEPA: request/enforce authorizations
  - PEPO: enforce obligations
- **PDP** (Policy Decision Point): evaluate ABAC policies
- **PIP** (Policy Information Point): collect attribute values
- **CH** (Context Handler): context enrichment

NIST National Institute of Standards and Technology U.S. Department of Commerce

ETSI

OASIS Advancing open standards for the information society

2002:
- First industrial applications of ABAC: Sun, Entrust, Oracle, IBM and others

2003:
- ABAC is standardized in XACML V1.0

2005:
- XACMLV2.0 and seven profiles (including SAML, RBAC, Privacy, etc.)

2009
- XPSA Profiles for Healthcare

2013
- Updated with major features to XACML v3.0

2014
- Updated profiles including drafts for REST, JSON, Administration & Delegation
- New profiles for Export Control, Intellectual Property, etc.
- NIST & NCCoE report endorses ABAC

2015:
- ALFA profile (draft)

2017:
- XACML v3.0 update

2019:
- XACML REST & JSON profile updates
- NIST & NCCoE reports re-endorses ABAC

Commercial:
NTT / Axiomatics Federal
Axiomatics (Nordea, PayPal, BoA, Bell H, …)
Next Labs (SAP, BAE Systems, Siemens, Microsoft, …)
Oracle, Atos, Ping. Empower ID,, PlainID, Symphonic, WSO2

Open source:
Balana, AuthZForce, FIWARE IDM, …

HUAWEI

ALFA/XACMLv3

XACML v3.0 : Current OASIS/NIST standard

Pros:

- Industry standard
- Widely used (NIST, NTT, Axiomatics, Oracle, PayPal, WSO2, etc)
- Baseline for many other standards in eHealth, eGov, etc.
- XML based
- Machine readable
- Extensible
- Clearly defined schema (programmable meta-model)
- Can support many complex scenarios

Cons:

- Verbose / long policies
- XML parsing overhead
- Complex data structures

ALFA: emerging industry standard & OASIS draft profile

Pros:

- Emerging industry standard profile (DRAFT)
- Supported by industry leader Axiomatics
- Can be translated to XACML v3.0 automatically
- Fast to parse and process
- Concise and optimized for common/typical access scenarios
- Easy to understand by developers
- Similar spirit to Rego policy language of OPA incubator of CNF

Cons:

- Few implementations
- No independent schematic representation (programmable meta-model)

```
<xacml3:Rule RuleId="f6637b3f-3690-4cce-989c-2ce9c053d6fa" Effect="Deny">
    <xacml3:Description>Use it or lose it: this policy denies access if lastLogin is more than 30 days away from today's
date</xacml3:Description>
    <xacml3:Target/>
    <xacml3:Condition >
        <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
            <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-than"/>
            <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:dateTime-add-dayTimeDuration">
                <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-only">
                    <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="com.acme.user.lastLogin" DataType="http://www.w3.org/2001/XMLSchema#dateTime" MustBePresent="false"/>
                </xacml3:Apply>
                <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#dayTimeDuration">P30D</xacml3:AttributeValue>
            </xacml3:Apply>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime" DataType="http://www.w3.org/2001/XMLSchema#dateTime"
MustBePresent="false"/>
        </xacml3:Apply>
    </xacml3:Condition>
</xacml3:Rule>
```

```
namespace example{
    policy article{
        target clause itemType=="article"
        apply firstApplicable
        rule editArticle{
            target clause actionId == "edit" and userRole == "editor"
            permit
            condition userId == owner
        }
    }
}
```

Resources about UCON+

- T. Dimitrakos, T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosett, A. Saracino, "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1801-1812
- A. Hariri, S. Bandopadhyay, A. Rizos, T. Dimitrakos, B. Crispo, and M. Rajarajan, "SIUV: A Smart Car Identity Management and Usage Control System Based on Verifiable Credentials," in ICT Systems Security and Privacy Protection, vol. 625, A. Jsang, L. Futcher, and J. Hagen, Eds. Cham: Springer International Publishing, 2021, pp. 36-50. doi: 10.1007 /978-3-030-78120-0_3.
- S. Bandopadhyay et al., "DataPAL: Data Protection and Authorization Lifecycle framework," 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2021, pp. 1-8, doi: 10.1109/SEEDA-CECNSM53056.2021.9566212.

HUAWEI

Pointers about ODRL In EDC

- EDC is trying to extend the support has also some differences
  - https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/873
  - https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/blob/5ee32800072a267260d2867a32adbe0426de0f5a/docs/Policies.md
- EDC transforms IDS to EDC policies
  - https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/tree/e200d9ec52c501bb803f57fa66441a54f04abba0/data-protocols/ids/ids-transform-v1/src/main/java/org/eclipse/dataspaceconnector/ids/transform
- New EDC take on policies
  - https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/issues/855
- IDSA Model Templates
  - https://github.com/International-Data-Spaces-Association/InformationModel/tree/develop/examples/contracts-and-usage-policy/templates

ODRL resources

- W3C standard for describing digital rights:
  - ODRL Information Model https://www.w3.org/TR/odrl-model/
  - ODRL Vocabulary and Expression https://www.w3.org/TR/odrl-vocab/
  - ODRL Best practices https://w3c.github.io/odrl/bp/
  - ODRL validator -http://odrlapi.appspot.com/ Java code
  - ODRL evaluator - https://github.com/nitmws/odrl-wprofile-evaltest1

https://wiki.acumos.org/pages/viewpage.action?pageId=20547401