Semantic Attribute-Based Access Control

An overview of the existing approaches

Hamed Arshad

Department of Informatics
University of Oslo

March 2018

Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)

Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs ***Access control***

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

  Authentication vs ***Access control***

- **Authentication**: Who goes there?

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

  Authentication vs ***Access control***

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs ***Access control***

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system
- **Access control**: Are you allowed to do that?

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs ***Access control***

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system
- **Access control**: Are you allowed to do that?
  - Restrictions on actions of authenticated users

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs ***Access control***

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system
- **Access control**: Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Access control enforced by

Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs ***Access control***

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system
- **Access control**: Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Access control enforced by
  - Access Control Lists
  - Capabilities
  - ...

Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)

Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC

Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes

Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC

Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC

Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC
- The XACML standard

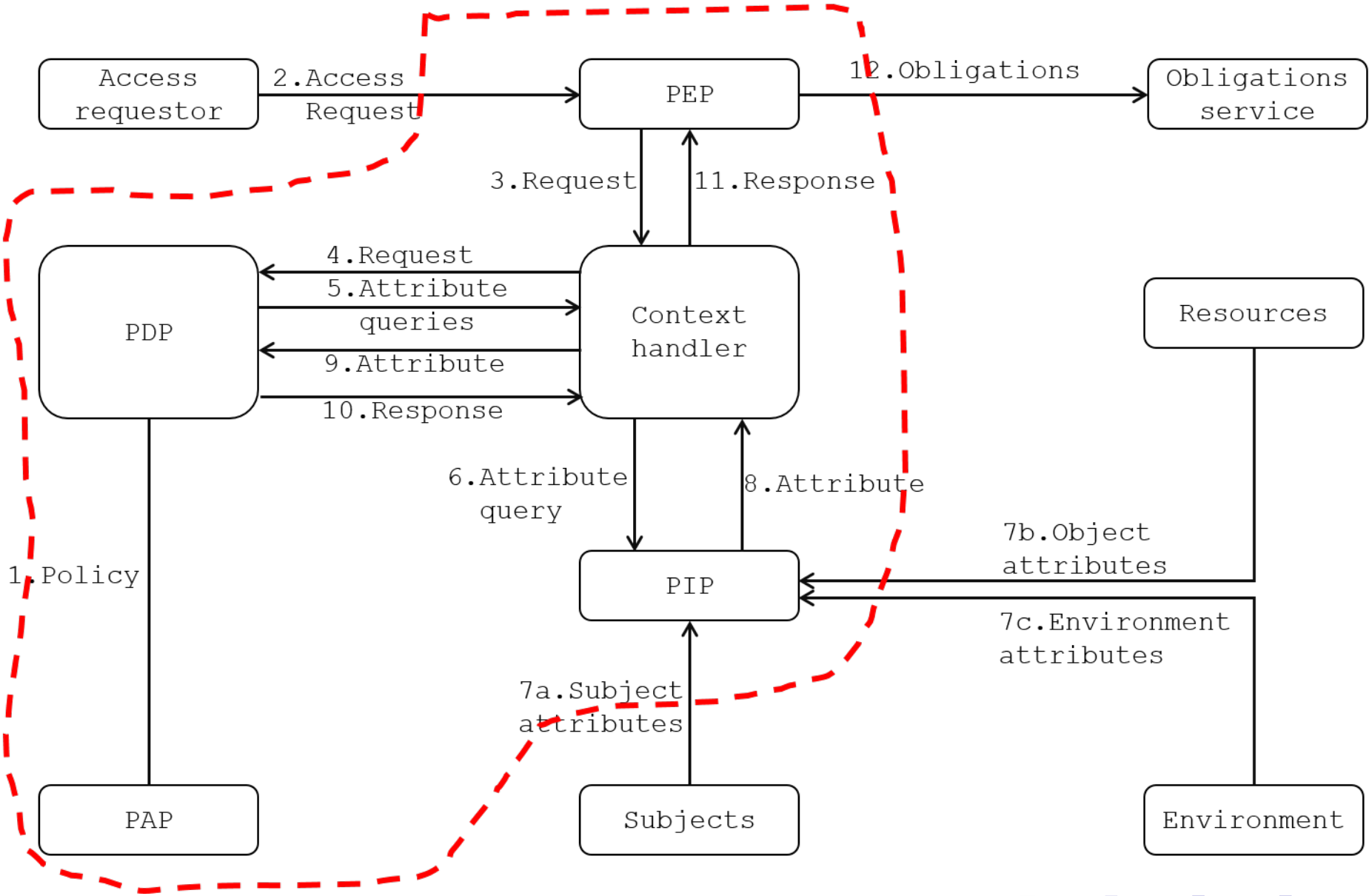
Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC
- The XACML standard
  - a policy language, which is sufficiently fine-grained and declarative

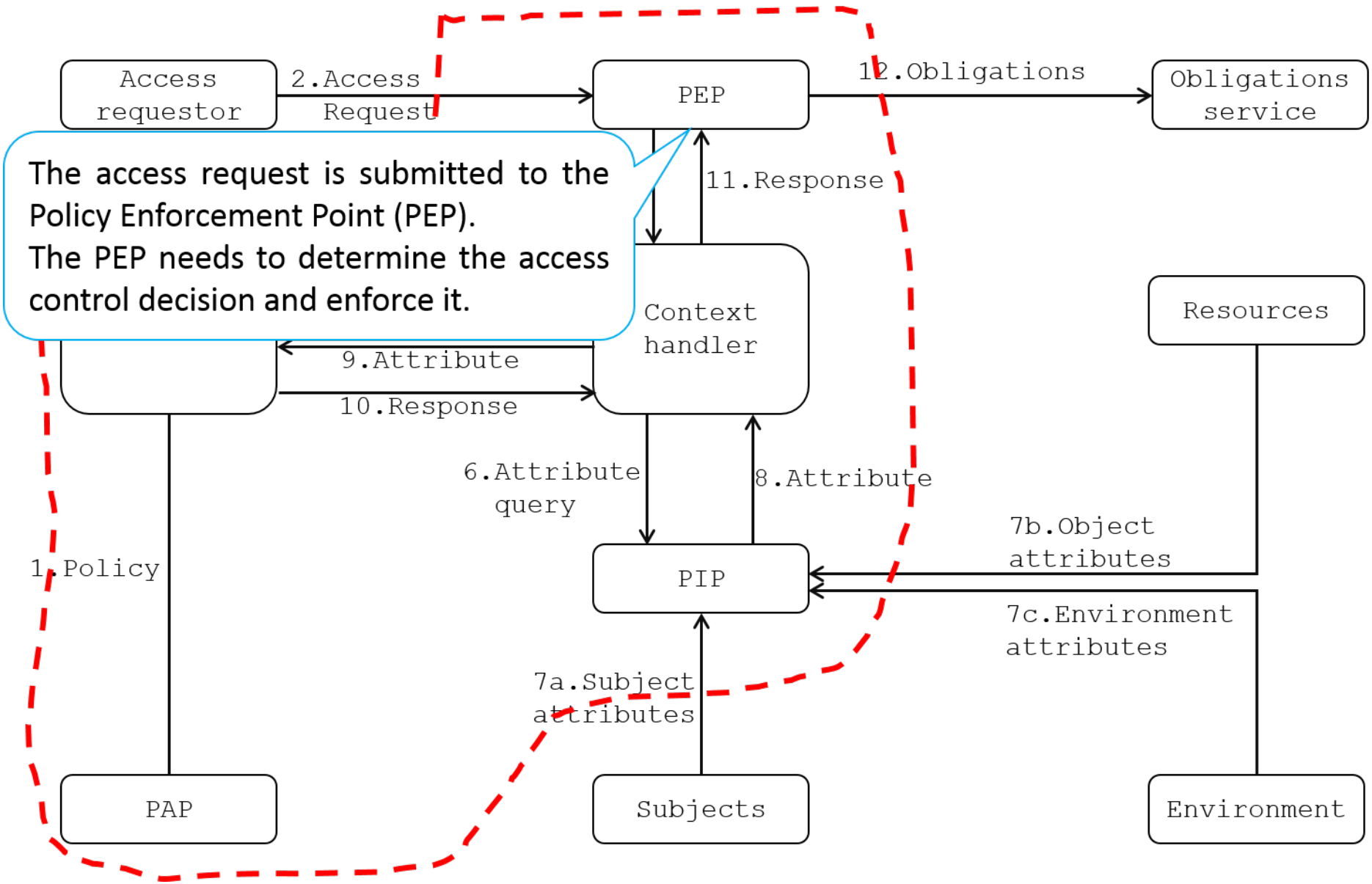
Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC
- The XACML standard
  - a policy language, which is sufficiently fine-grained and declarative
  - as well as an architecture for ABAC

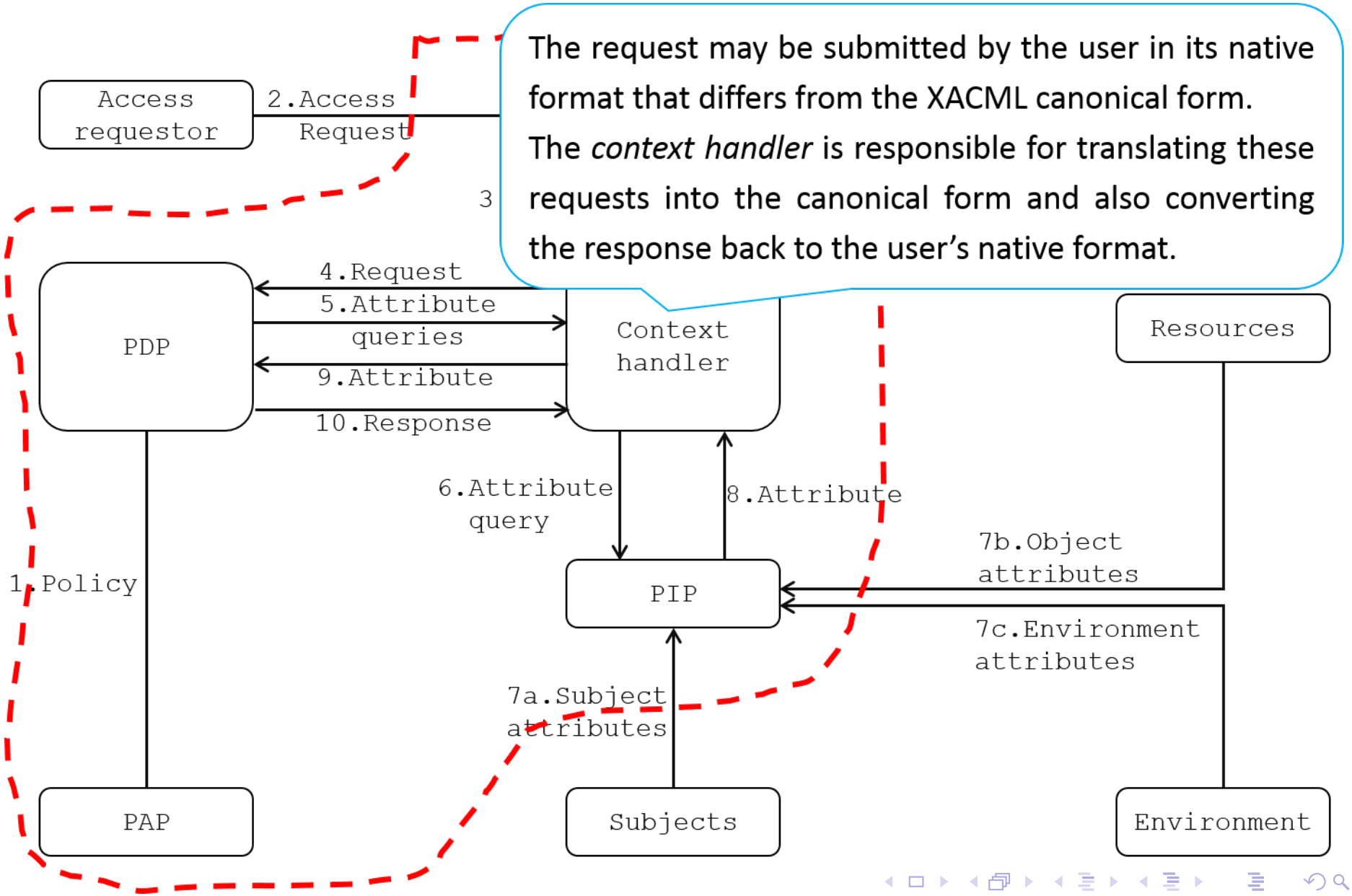
Attribute-Based Access Control (ABAC)



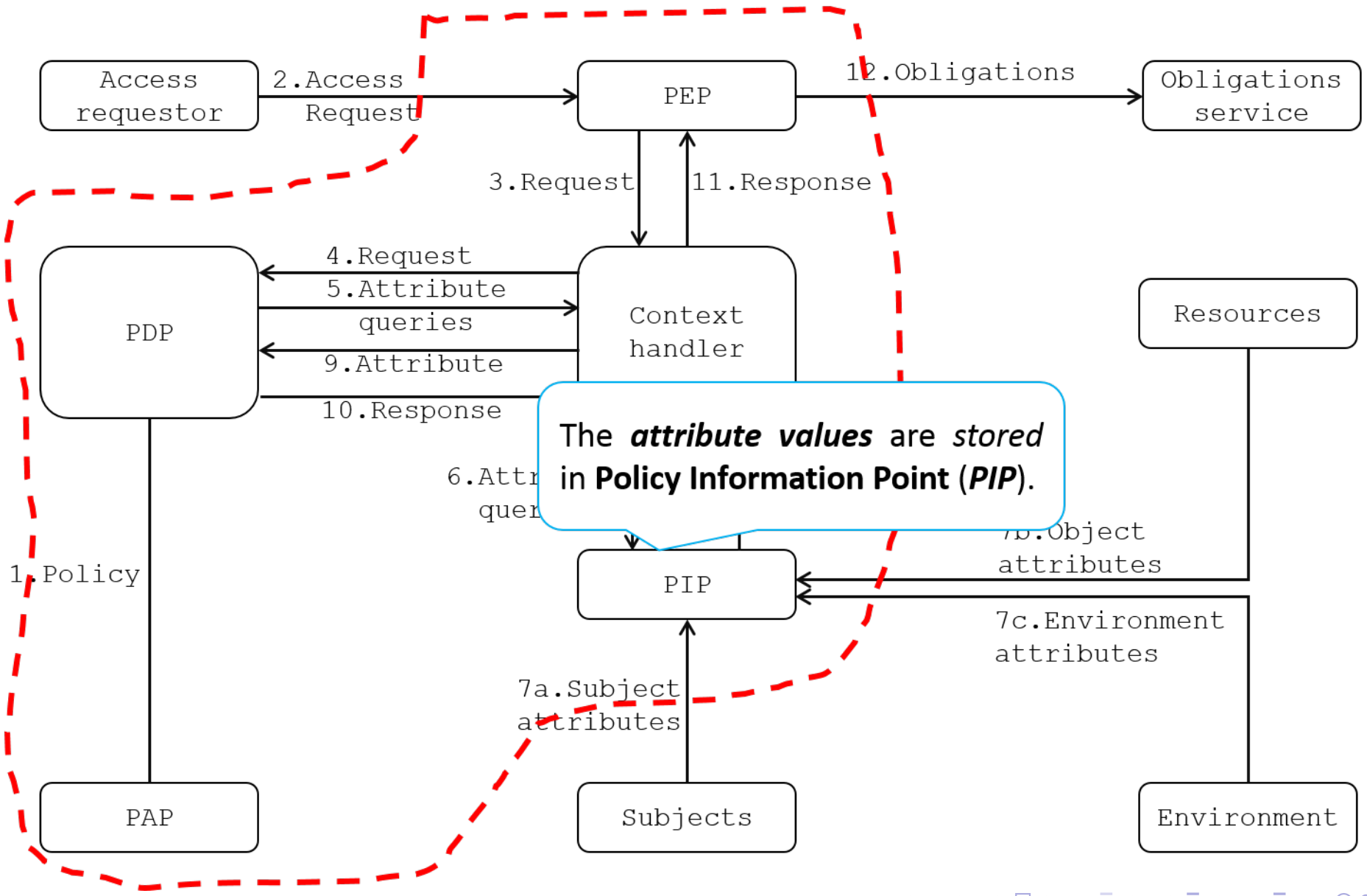
Attribute-Based Access Control (ABAC)



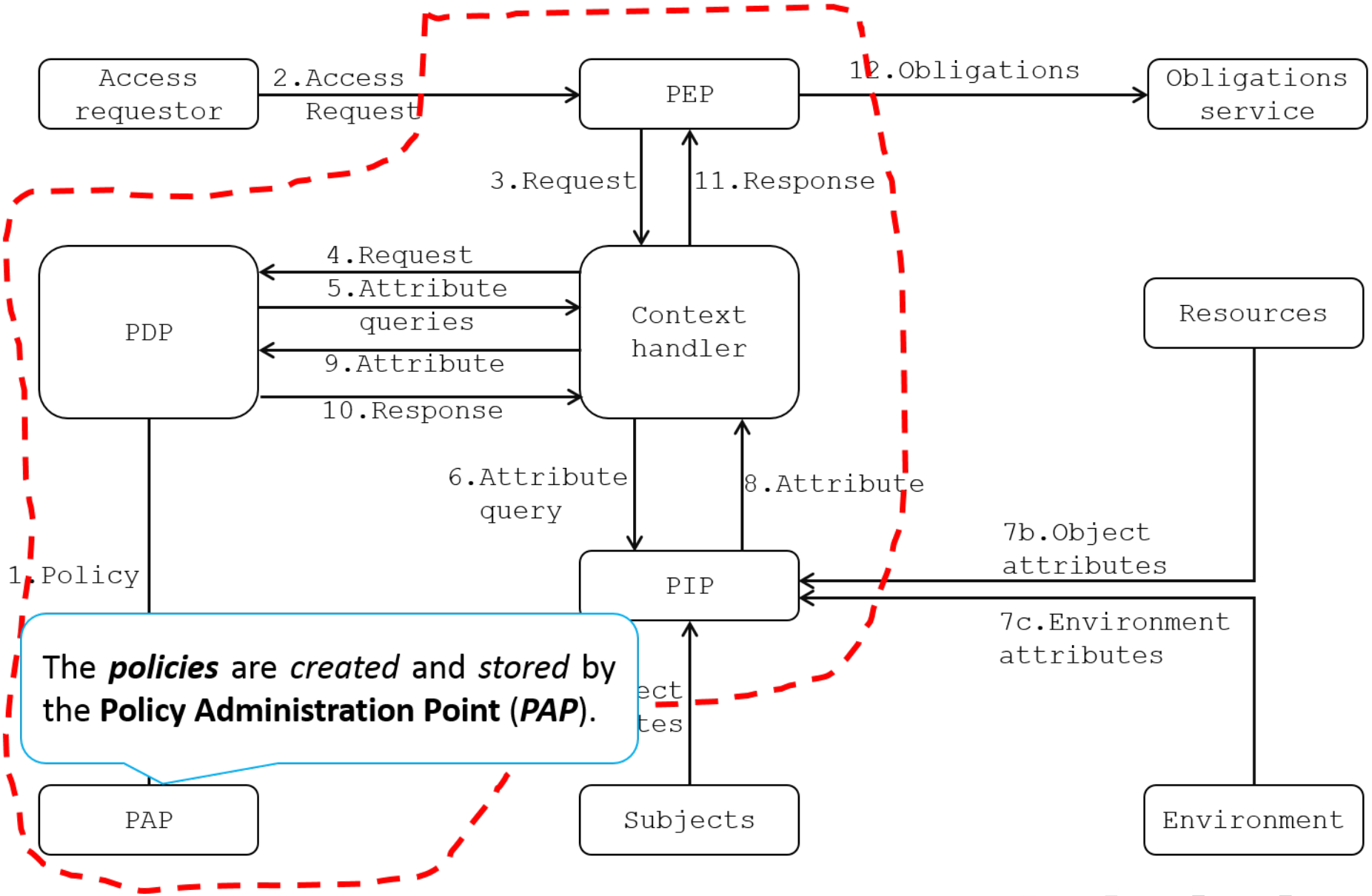
Attribute-Based Access Control (ABAC)



Attribute-Based Access Control (ABAC)

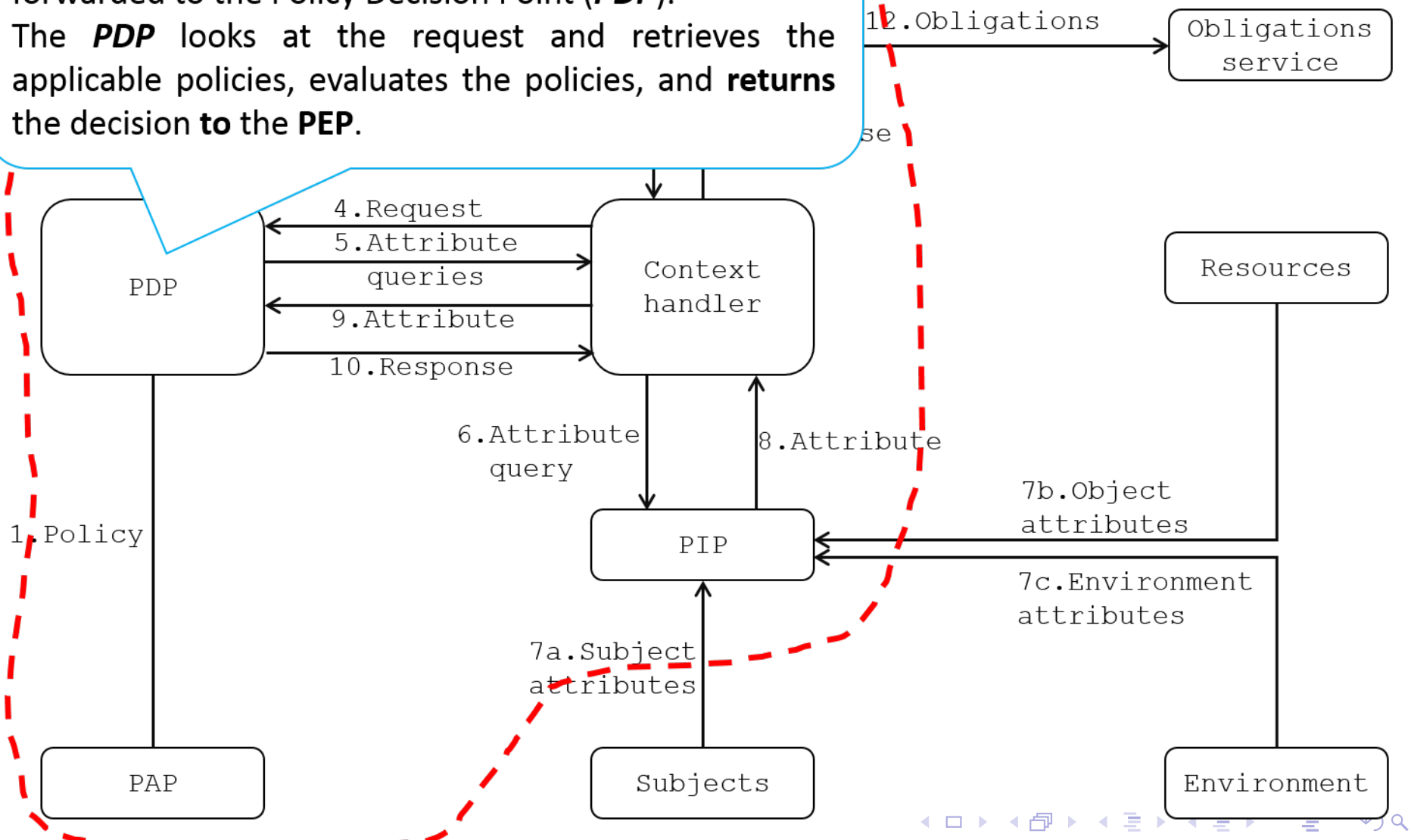


Attribute-Based Access Control (ABAC)



Attribute-Based Access Control (ABAC)

The request, converted by the context handler, is forwarded to the Policy Decision Point (***PDP***).
The ***PDP*** looks at the request and retrieves the applicable policies, evaluates the policies, and **returns** the decision **to** the **PEP**.



Attribute-Based Access Control (ABAC)

```
<?xml version="1.0" encoding="UTF-8"?>
- <PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides" Version="2.0" PolicySetId="root"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17 http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
    <Target/>
  - <Policy Version="1.0" xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17 http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides" PolicyId="urn:oasis:names:tc:xacml:3.0:example:MyPolicy">
      <Target/>
    - <Rule Effect="Permit" RuleId="urn:oasis:names:tc:xacml:3.0:example:MyRule">
      - <Target>
        - <AnyOf>
          - <AllOf>
            - <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Medical record</AttributeValue>
                <AttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" MustBePresent="false"/>
              </Match>
            - <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Doctor</AttributeValue>
                <AttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" MustBePresent="false"/>
              </Match>
            </AllOf>
          </AnyOf>
        </Target>
      - <Condition>
        - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
              <AttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action" MustBePresent="false"/>
            </Apply>
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
          </Apply>
        </Condition>
      </Rule>
      <Rule Effect="Deny" RuleId="DenyRule"/>
    </Policy>
</PolicySet>
```

Attribute-Based Access Control (ABAC)

```
<PolicySet PolicySetId = "PolicySetInstitute1" policy-combining-algorithm="permit-overrides">
<Target>
/*:Attribute-Category :Attribute ID :Attribute Value */
AnyOf :access-subject
      :access-subject :Role       :Researcher
      :access-subject :Role       :Doctor
AnyOf :resource
      :resource   :Type     :HealthData
      :resource   :Type     :AggregateHealthData
AnyOf :action
      :action     :Action-id      :Release
      :action     :Action-id      :Read
      :action     :Action-id      :Write
</Target>
<Policy PolicyId ="Policy1" rule-combining-algorithm="deny-overrides">
// Institute 1 Rules //
<Target>
/* :Attribute-Category :Attribute ID :Attribute Value */
:access-subject         :Role     :Researcher
AnyOf :resource
      :resource   :Type     :HealthData
      :resource   :Type     :AggregateHealthData
:action           :Action-id      :Release
</Target>
<Rule RuleId = "I1R1" Effect="Permit">
<Condition>
Function: string-equal
/* :Attribute-Category :Attribute ID :Attribute Value */
:access-subject :HIPAA Comp     :Yes
</Condition>
</Rule>
</Policy>
</PolicySet>
```

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***
- Considering all the possible synonyms (semantically) of each attribute

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy
  - a large number of manual work

Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in ***open and distributed systems***
- ***Heterogeneous*** systems = ***mismatch*** between attributes

Example

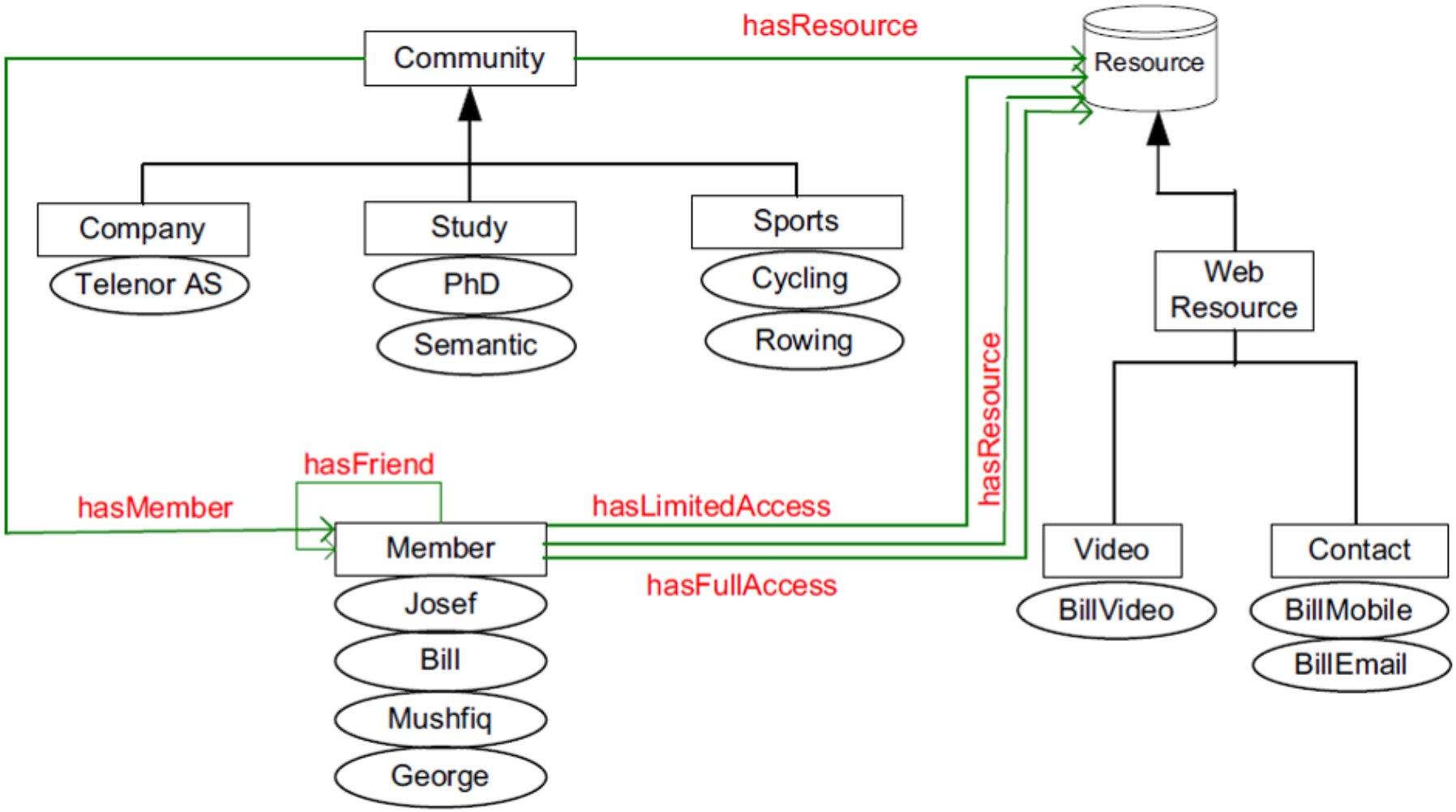
- An e-healthcare system may represent adult patients with an attribute ***"Adult"***
- Patients may try to prove using ***"hasDriverLicense"*** or ***"age"***
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy
  - a large number of manual work

ABAC needs to be extended

Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)

Semantic-Based Access Control (SBAC)



The description of the ontology using classes, properties and instances

Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)

Semantic Attribute-Based Access Control (SABAC)

- Idea: ABAC + semantic technologies

Semantic Attribute-Based Access Control (SABAC)

- Idea: ABAC + semantic technologies
  - making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones

Semantic Attribute-Based Access Control (SABAC)

- Idea: ABAC + semantic technologies
  - making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones
- Formally define entities and their attributes and relationships using an ontology

Semantic Attribute-Based Access Control (SABAC)

- Idea: ABAC + semantic technologies
  - making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones
- Formally define entities and their attributes and relationships using an ontology
- Describing relations for specific conditions using rule markup languages

Semantic Attribute-Based Access Control (SABAC)

- Separation of ***ontology*** management from ***access*** management

Semantic Attribute-Based Access Control (SABAC)

- Separation of ***ontology*** management from ***access*** management
- Two parts:
  - An ontology management system

Semantic Attribute-Based Access Control (SABAC)

- Separation of ***ontology*** management from ***access*** management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes

Semantic Attribute-Based Access Control (SABAC)

- Separation of ***ontology*** management from ***access*** management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes
  - An access control system

Semantic Attribute-Based Access Control (SABAC)

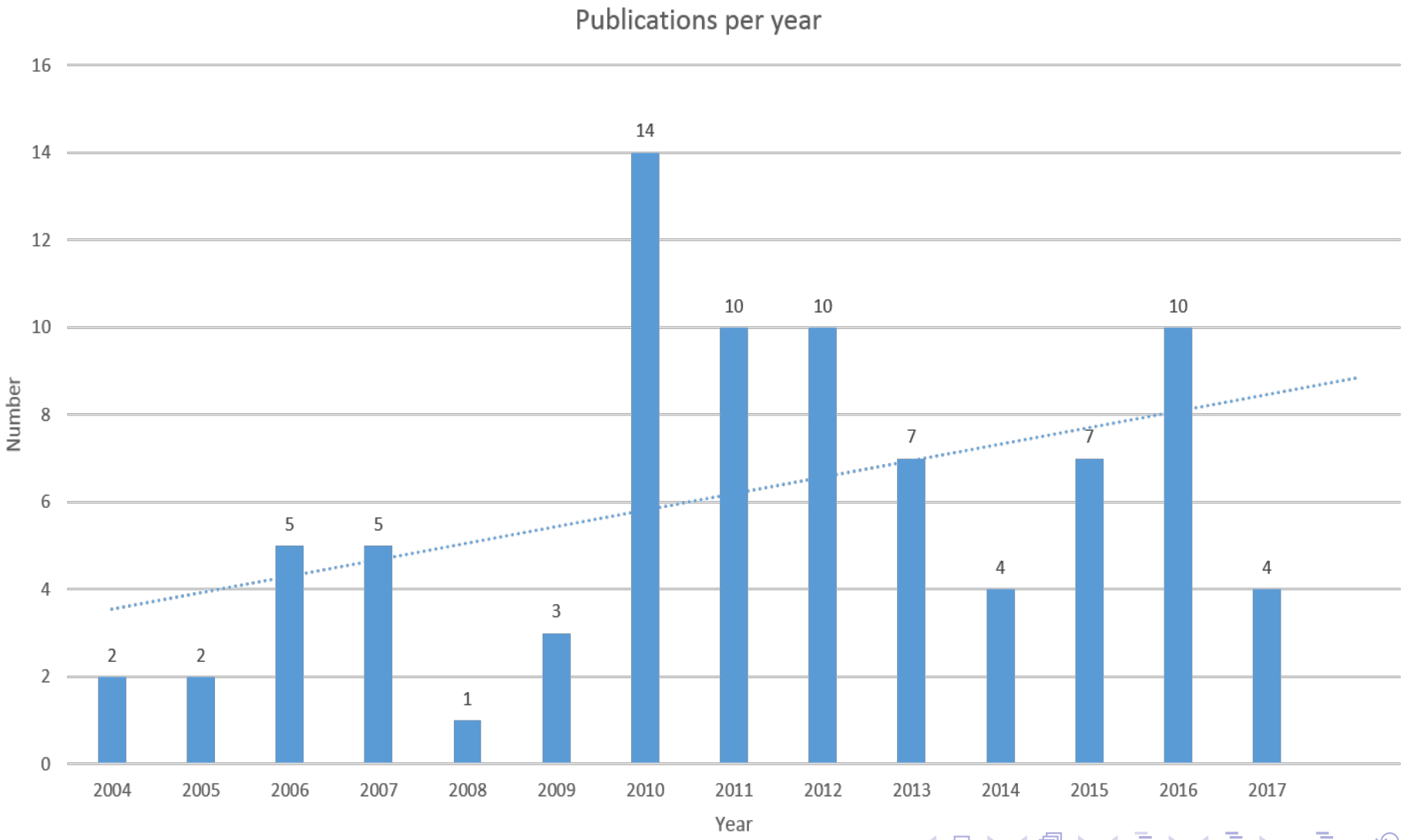
- Separation of ***ontology*** management from ***access*** management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes
  - An access control system
    - uses the extended attributes for access evaluation

Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?

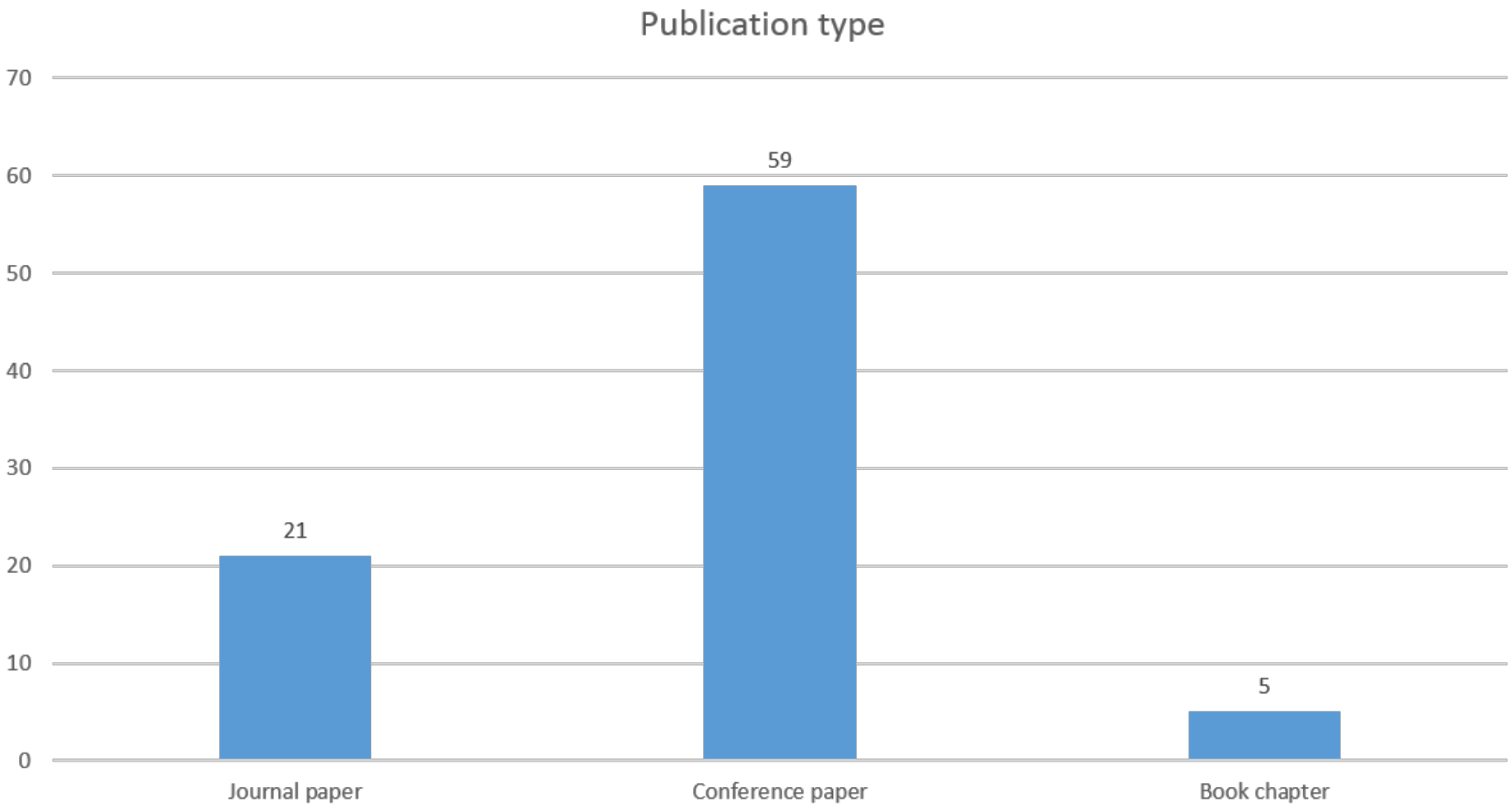
Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?



Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?



Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?

Title	Year	Journal
Multi-level authorisation model and framework for distributed semantic-aware environments	2010	IET Information Security
Utilizing Semantic Knowledge for Access Control in Pervasive and Ubiquitous Systems	2010	Mobile Networks and Applications
Ontology based policy interoperability in geo-spatial domain	2011	Computer Standards & Interfaces
Privilege Management Infrastructure for Virtual Organizations in Healthcare Grids	2011	IEEE Transactions on Information Technology in Biomedicine
Semantics-based Access Control Approach for Web Service	2011	Journal of Computers
A semantic approach for fine-grain access control of e-health documents	2012	Logic Journal of IGPL
Building and evaluating an ontology-based tool for reasoning about consent permission	2013	AMIA Annu Symp Proc
Extensible access control markup language integrated with Semantic Web technologies	2013	Information Sciences
A SEMANTIC SECURITY FRAMEWORK FOR SYSTEMS OF SYSTEMS	2013	International Journal of Cooperative Information Systems
Empowering citizens with access control mechanisms to their personal health resources	2013	International Journal of Medical Informatics
Secure Semantic Aware Middleware: a Security Based Semantic Access Control for Web Services	2013	International Review on Computers and Software (IRECOS)
Sophisticated Access Control via SMT and Logical Frameworks	2014	ACM Transactions on Information and System Security (TISSEC)
Fine-grained filtering to provide access control for data providing services within collaborative environments	2015	Concurrency and Computation: Practice & Experience
A Combination of Semantic andAttribute-based Access Control Model for Virtual Organizations	2015	The ISC International Journal of Information Security (ISeCure)
A HIGH PERFORMANCE UCON AND SEMANTIC-BASED AUTHORIZATION FRAMEWORK FOR GRID COMPUTING	2016	Journal of Information & Communication Technology
Access Control as a Service for Information Protection in Semantic Web based Smart Environment	2016	Journal of Internet Computing and Services
Semantically Enriched Data Access Policies in eHealth	2016	Journal of Medical Systems
PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services	2017	Journal of Grid Computing
Semantic Based Authorization Framework For Multi-Domain Collaborative Cloud Environments	2017	Procedia Computer Science
Semantic privacy-preserving framework for electronic health record linkage	2017	Telematics and Informatics
Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in	2018	Future Generation Computer Systems

Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?

Title	Year	Conference
Extending Policy Languages to the Semantic Web	2004	Web Engineering 4th International Conference, ICWE 2004
Supporting Attribute-based Access Control with Ontologies	2006	Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on
Exhtending Policy Languages to the Semantic Web	2004	International Conference on Web Engineering, ICWE 2004: Web Engineering
Securing Web Services Using Semantic Web Technologies	2005	IFIP Working Conference on Industrial Applications of Semantic Web
New paradigms for access control in open environments	2005	Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on
Description Logic Modeling of Temporal Attribute-Based Access Control	2006	Communications and Electronics, 2006. ICCE '06. First International Conference on
A Unified Access Control Infrastructure Using Attributes and Ontology in E-Learning Resource Grids	2006	Computational Intelligence and Security, 2006 International Conference on
Provenance Explorer – Customized Provenance Views Using Semantic Inferencing	2006	International Semantic Web Conference. ISWC 2006: The Semantic Web - ISWC 2006
Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies	2006	Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006)
Enforcing Privacy by Means of an Ontology Driven XACML Framework	2007	Information Assurance and Security, 2007. IAS 2007. Third International Symposium on
Building a Distributed Semantic-aware Security Architecture	2007	New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007. IFIP International Federation for Information Processing
A Role and Attribute Based Access Control System Using Semantic Web Technologies	2007	OTM'07 Proceedings of the 2007 OTM Confederated international conference on On the move to meaningful internet systems
Using semantics for automatic enforcement of access control policies among dynamic coalitions	2007	SACMAT '07 Proceedings of the 12th ACM symposium on Access control models and technologies
Semantic-Based Access Control for Grid Data Resources in Open Grid Services Architecture - Data Access and Integratic	2008	20th IEEE International Conference on Tools with Artificial Intelligence
Description Logic and Subject Attribute Based Grid Authorization Model	2009	Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on
A Semantic-Aware Attribute-Based Access Control Model for Web Services	2009	International Conference on Algorithms and Architectures for Parallel Processing ICA3PP 2009: Algorithms and Architectures for Parallel Processing
Supporting RBAC with XACML+OWL	2009	SACMAT '09 Proceedings of the 14th ACM symposium on Access control models and technologies
Attribute Mapping for Cross-Domain Access Control	2010	Computer and Information Application (ICCIA), 2010 International Conference on
Enabling Privacy-preserving Credential-based Access Control with XACML and SAML	2010	Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on
dynamic context-aware information access in virtual organizations	2010	Computing in Civil and Building Engineering, Proceedings of the International Conference
Fine-grained information access in Virtual Organisations	2010	eChallenges
XML secure views using semantic access control	2010	EDBT '10 Proceedings of the 2010 EDBT/ICDT Workshops
A New Trust Degree-Based Access Control Method for Semantic Web Services	2010	Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on
A Semantic- and Attribute-Based Framework for Web Services Access Control	2010	Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on
A Semantic Security Architecture for Web Services The Access-eGov Solution	2010	International Conference on Availability, Reliability and Security
Extending XACML Profile for RBAC with Semantic Concepts	2010	International Conference on Computer Application and System Modeling (ICCASM 2010)
Concept Alignment in Attribute Based Access Control	2010	International Conference on Multimedia Information Networking and Security
Towards Semantic Matching of Attributes in Multi-domain Access Control	2010	International Symposium on Intelligence Information Processing and Trusted Computing
Ontology-based Access Control Policy Interoperability	2010	Proc. 1st Conference on Mobility, Individualisation, Socialisation and Connectivity, MISC
A Context-Aware Semantic-Based Access Control Model for Mobile Web Services	2011	Advanced Research on Computer Science and Information Engineering
APHR: Annotated Personal Health Record for Enabling Pervasive Healthcare	2011	Mobile Data Management (MDM), 2011 12th IEEE International Conference on
Ontology Based Interoperation for Securely Shared Services: Security Concept Matching for Authorization Policy Interop	2011	New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on
Ontology Based Interoperation for Securely Shared Services	2011	New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on
Ontology-Based Matching of Security Attributes for Personal Data Access in e-Health	2011	OTM Confederated International Conferences "On the Move to Meaningful Internet Systems". OTM 2011: On the Move to Meaningful Internet Systems: OTM 2011
Realization Distributed Access Control Based on Ontology and Attribute with OWL	2012	Advances in Electronic Engineering, Communication and Management
Fast semantic Attribute-Role-Based Access Control (ARBAC) in a collaborative environment	2012	Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on
Semantic access control for cloud computing based on e-Healthcare	2012	Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on
X-STROWL: A generalized extension of XACML for context-aware spatio-temporal RBAC model with OWL	2012	Digital Information Management (ICDIM), 2012 Seventh International Conference on
Fine-Grained Filtering of Data Providing Web Services with XACML	2012	Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2012 IEEE 21st International Workshop on
Ontological Approach for the Management of Informed Consent Permissions	2012	HISB '12 Proceedings of the 2012 IEEE Second International Conference on Healthcare Informatics, Imaging and Systems Biology
F-SAMS: Reliably Identifying Attributes and Their Identity Providers in a Federation	2012	OTM Confederated International Conferences "On the Move to Meaningful Internet Systems" OTM 2012: On the Move to Meaningful Internet Systems: OTM 2012 Workshops
An Attributes-Based Access Control Architecture within Large-Scale Device Collaboration Systems Using XACML	2012	Proceedings of the International Conference on Green Communications and Networks
Towards Semantic-Enhanced Attribute-Based Access Control for Cloud Services	2012	Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on
Web Service Semantic Access Control	2013	Innovative Computing Technology (INTECH), 2013 Third International Conference on
A Semantic Policy Framework for Context-Aware Access Control Applications	2013	Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on
A virtual PHR authorization system	2014	Biomedical and Health Informatics (BHI), 2014 IEEE-EMBS International Conference on
Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems	2014	Biomedical and Health Informatics (BHI), 2014 IEEE-EMBS International Conference on
Attribute-based Fine Grained Access Control for Triple Stores	2015	3rd Society, Privacy and the Semantic Web - Policy and Technology workshop, 14th International Semantic Web Conference
An OWL-based XACML Policy Framework	2015	e-Business and Telecommunications (ICETE), 2015 12th International Joint Conference on
Extensible privacy framework for Web of objects based ubiquitous services	2015	Information and Communication Technology Convergence (ICTC), 2015 International Conference on
Semantic Generation of Clouds Privacy Policies	2015	International Conference on Cloud Computing and Services Science
Ontology-Based Delegation of Access Control: An Enhancement to the XACML Delegation Profile	2015	International Conference on Trust and Privacy in Digital Business TrustBus 2015: Trust, Privacy and Security in Digital Business
Using OWL Reasoning for Evaluating XACML Policies	2016	International Conference on E-Business and Telecommunications. ICETE 2015: E-Business and Telecommunications
HBAC: An access control over Semantics-enabled Smart Grids to enable energy-efficiency and lifetime optimization	2016	International Conference on Information and Convergence Technology for Smart Society
An Ontology Regulating Privacy Oriented Access Controls	2016	International Conference on Risks and Security of Internet and Systems
Representing Attribute Based Access Control Policies in OWL	2016	Semantic Computing (ICSC), 2016 IEEE Tenth International Conference on
Context-Sensitive Policy Based Security in Internet of Things	2016	Smart Computing (SMARTCOMP), 2016 IEEE International Conference on
Semantic-Based Privacy Protection of Electronic Health Records for Collaborative Research	2016	Trustcom/BigDataSE/ISPA, 2016 IEEE
Graphical Interface for Ontology Mapping with Application to Access Control	2017	Asian Conference on Intelligent Information and Database Systems

Semantic Attribute-Based Access Control (SABAC)

- What has been done till now?

Title	Year	Book
Bringing Semantic Security To Semantic Web Services	2007	The Semantic Web: Real-World Applications from Industry, volume 6 of Semantic Web and Beyond
Semantic Similarity-Based Web Services Access Control	2011	Autonomous Systems: Developments and Trends
Semantic Mapping for Access Control Model	2011	Innovations in SMEs and Conducting E-Business: Technologies, Trends and Solutions
Ontology-Driven Authorization Policies on Personal Health Records for Sustainable Citizen-Centered	2014	Concepts and Trends in Healthcare Information Systems, Annals of Information Systems
Semantic Policy Information Point – preliminary considerations	2016	ICT Innovations 2015

Semantic Attribute-Based Access Control (SABAC)

The existing approaches can be categorized as:

Semantic Attribute-Based Access Control (SABAC)

The existing approaches can be categorized as:

- ***Hybrid models: ABAC + SBAC***
  - Amini et al. "A combination of semantic and attribute based access control model for virtual organizations," The ISC Int. J. of Inf. Sec., 2015.

Semantic Attribute-Based Access Control (SABAC)

The existing approaches can be categorized as:

- ***Hybrid models: ABAC + SBAC***
  - Amini et al. "A combination of semantic and attribute based access control model for virtual organizations," The ISC Int. J. of Inf. Sec., 2015.
- ***New policy languages***
  - Calvillo et al. "Privilege management infrastructure for virtual organizations in healthcare grids," IEEE Trans. on Inf. Tech. in Biomed., 2011.
  - Lu and Sinnott, "Semantic privacy-preserving framework for electronic health record linkage," Telematics and Informatics, 2017.
  - Amini and Jalili, "Multi-level authorisation model and framework for distributed semantic-aware environments," IET Inf. Sec., 2010.
  - Hsu, "Extensible access control markup language integrated with semantic web technologies," Inf. Sci., 2013.

Semantic Attribute-Based Access Control (SABAC)

The existing approaches can be categorized as:

- ***Hybrid models: ABAC + SBAC***
  - Amini et al. "A combination of semantic and attribute based access control model for virtual organizations," The ISC Int. J. of Inf. Sec., 2015.
- ***New policy languages***
  - Calvillo et al. "Privilege management infrastructure for virtual organizations in healthcare grids," IEEE Trans. on Inf. Tech. in Biomed., 2011.
  - Lu and Sinnott, "Semantic privacy-preserving framework for electronic health record linkage," Telematics and Informatics, 2017.
  - Amini and Jalili, "Multi-level authorisation model and framework for distributed semantic-aware environments," IET Inf. Sec., 2010.
  - Hsu, "Extensible access control markup language integrated with semantic web technologies," Inf. Sci., 2013.
- ***Extending the XACML architecture***
  - Priebe et al. "Supporting attribute-based access control with ontologies". In ARES 2006. IEEE.
  - Dersingh et al."Utilizing semantic knowledge for access control in pervasive and ubiquitous systems," Mob. Net. & App., 2010.
  - Drozdowicz et al. "Semantically enriched data access policies in ehealth," J. of med. sys., 2016.
  - Damiani et al. "Extending policy languages to the semantic web," in Int. Conf. on Web Eng., 2004.
  - Hilia et al. "Semantic based authorization framework for multi-domain collaborative cloud environments," Procedia Com. Sci., 2017.

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies

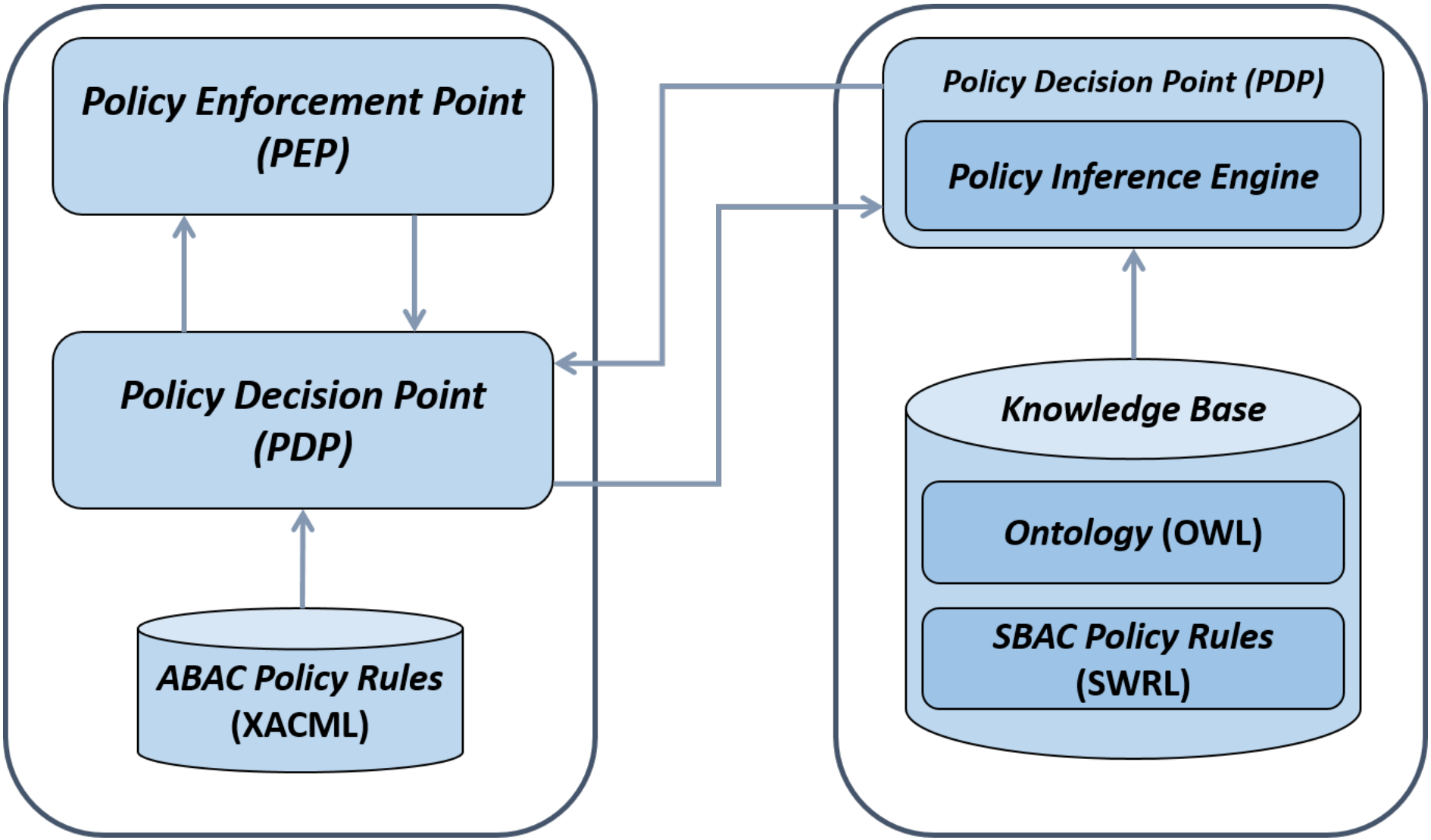
Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies
    - The ontology has two basic concepts (Subject and Object) and two basic relations (Permission and Prohibition)

Semantic Attribute-Based Access Control (SABAC)

- ***Hybrid models: ABAC + SBAC***
  - A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies
    - The ontology has two basic concepts (Subject and Object) and two basic relations (Permission and Prohibition)

Semantic Attribute-Based Access Control (SABAC)



Semantic Attribute-Based Access Control (SABAC)

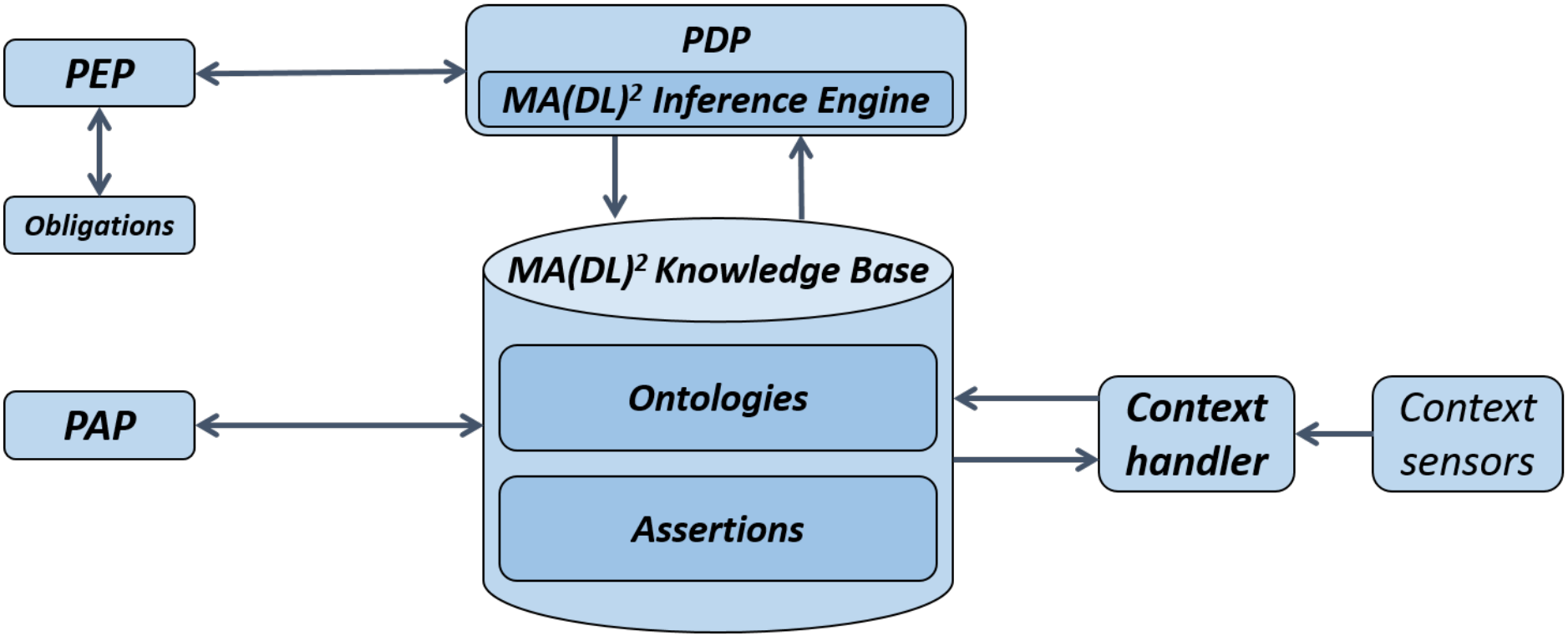
- ***New policy languages***

Semantic Attribute-Based Access Control (SABAC)

- ***New policy languages***
  - $MA(DL)^2$ logic for policy specification and inference

Semantic Attribute-Based Access Control (SABAC)

- ***New policy languages***
  - $MA(DL)^2$ logic for policy specification and inference



Semantic Attribute-Based Access Control (SABAC)

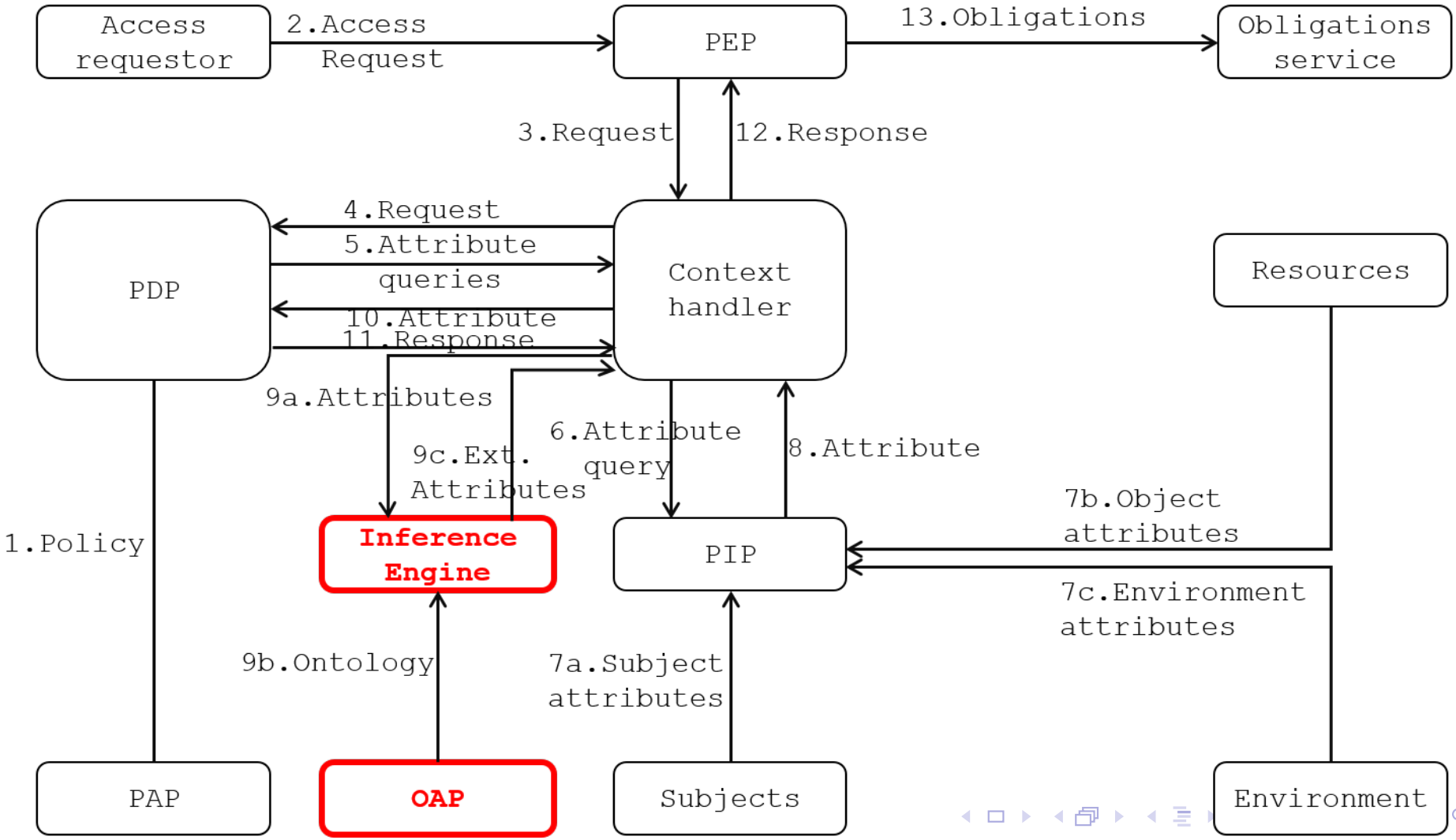
- ***Extending the XACML architecture***

Semantic Attribute-Based Access Control (SABAC)

- ***Extending the XACML architecture***
  - Adding a component to the architecture

Semantic Attribute-Based Access Control (SABAC)

- ***Extending the XACML architecture***
  - Adding a component to the architecture



Thank you!