

Constrained Delegation for XML-based Access Control and Digital Rights Management Standards

Guillermo Navarro, Babak Sadighi Firozabadi, Erik Rissanen, Joan Borrell

gnavarro@ccd.uab.es

Policy Based Reasoning Group,
Swedish Institute of Computer Science (SICS)

Combinatorics and Digital Communication Group
Universitat Autònoma de Barcelona.

Contents

- ▶ Constrained delegation model
- ▶ XML-based Access Control and Digital Rights Management Standards (SAML, XACML, XrML) and constrained delegation.
- ▶ Conclusions.

Delegation for AC and DRM

Delegation \implies **decentralized management** of Access Control and Digital Rights Management.

- ▶ Decision makers can implement their decisions.
- ▶ Increases the level of security.
- ▶ Corresponds to the actual authority and responsibility structures.

Constrained Delegation Model

Constrained Delegation model (*Sadighi et al. 2002, Bandmann et al. 2003*)

- ▶ Delegation in terms of creating new permissions and authorities.

authority to create a permission \neq make use of the permission

- ▶ Delegation chains can be constrained at each step of delegation.
- ▶ A valid chain originates from a source of authority.

XML-based Standards for Access Control

- ▶ Secure Assertion Markup Language (SAML):
 - ▷ Framework for exchanging authentication and authorization information.
 - ▷ OASIS standard (v1.1), Sept. 2003.

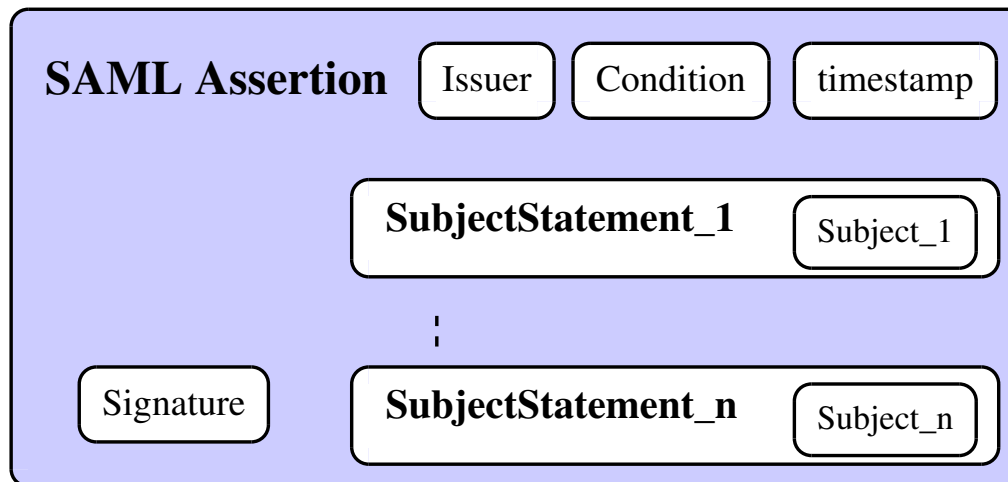
XML-based Standards for Access Control

- ▶ Secure Assertion Markup Language (SAML):
 - ▷ Framework for exchanging authentication and authorization information.
 - ▷ OASIS standard (v1.1), Sept. 2003.
- ▶ eXtensible Access Control Markup Language (XACML):
 - ▷ Language for describing access control policies and a request/response protocol.
 - ▷ OASIS standard (v1.0), Febr. 2003.

XML-based Standards for DRM

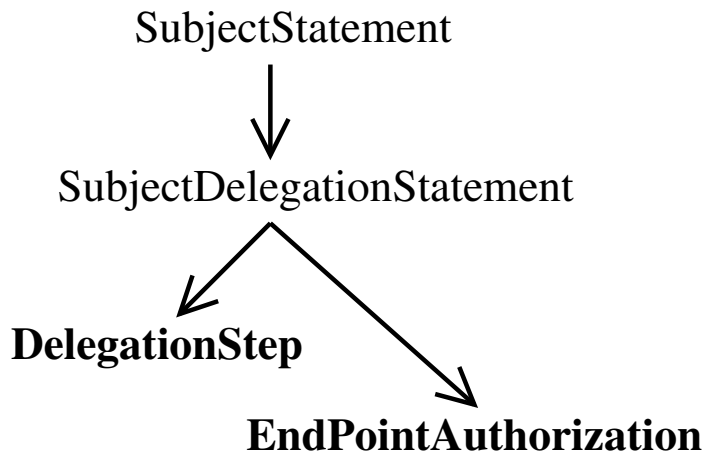
- ▶ eXtensible rights Markup Language (XrML):
 - ▷ Language for specifying and managing rights to control the access to digital content and services.
 - ▷ Specification by ContentGuard (v2.0) Nov. 2003.
 - ▷ Considered by some standardization organizations: MPEG-21 REL (Rights Expression Language) (MPEG working group (ISO/IEC)), Open eBook Rights and Rules Working Group (RRWG) (Open eBook Forum).

Secure Assertion Markup Language (SAML)



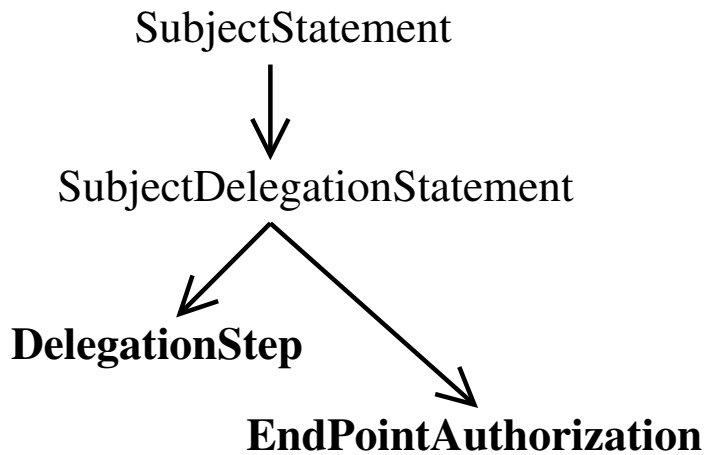
- ▶ **SAML assertion:** a statement (or declaration of facts) about a subject made by an issuer.
- ▶ Statements: SubjectStatement, AuthenticationStatement, AuthorizationDecisionStatement, and AttributeStatement.
- ▶ **Delegation is not supported** by the SAML specification (v1.1).

SAML delegation

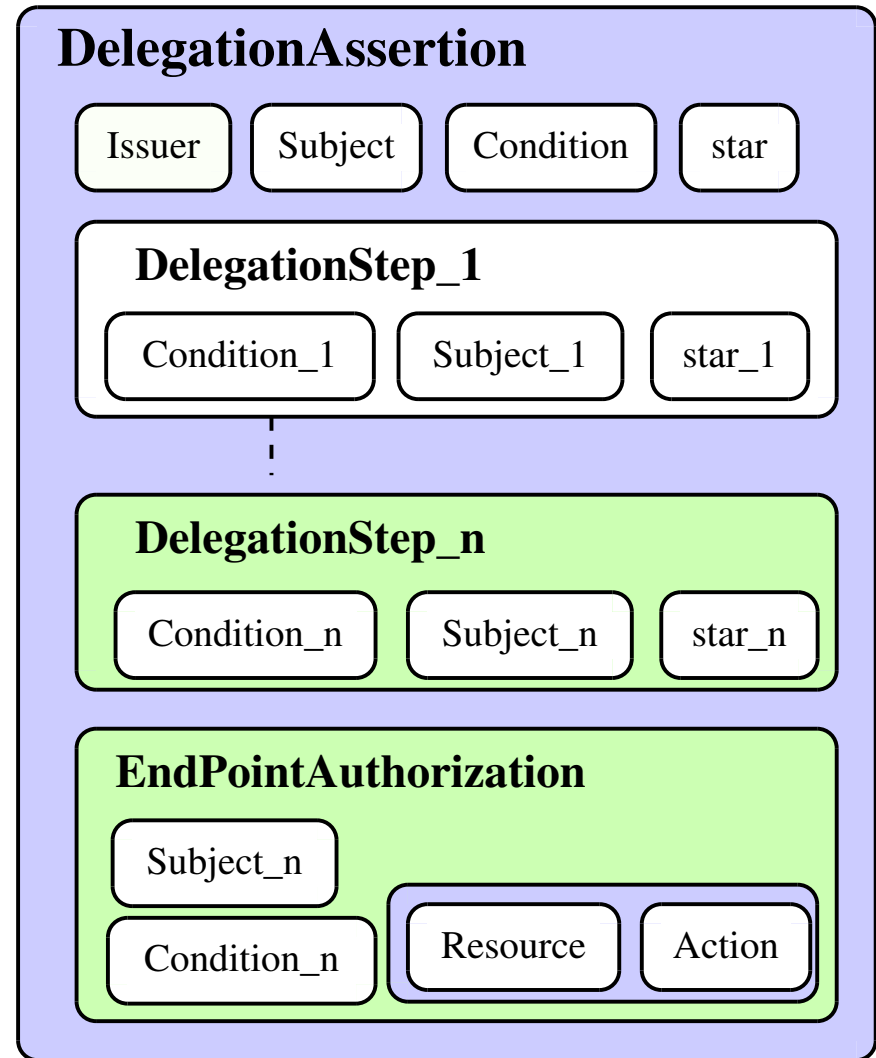


- ▶ New **subject** statements.
- ▶ Allows the specification of a full delegation chain.

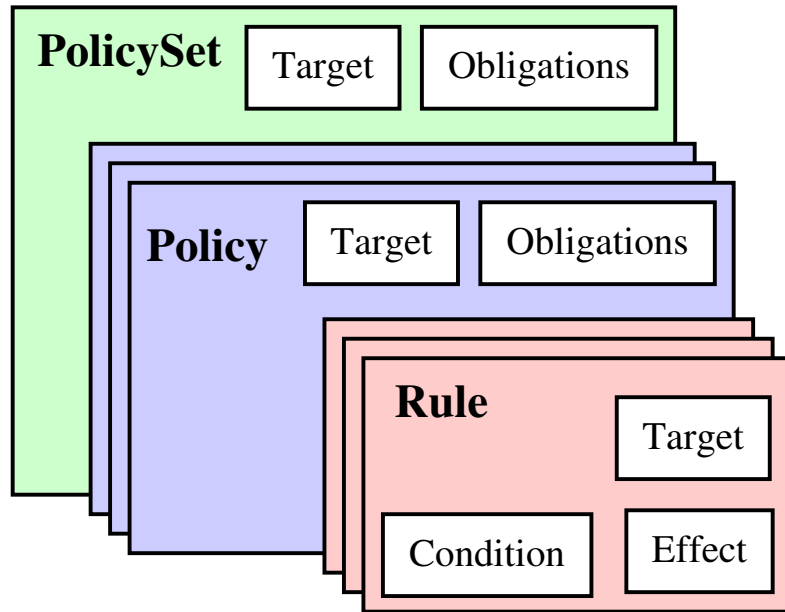
SAML delegation



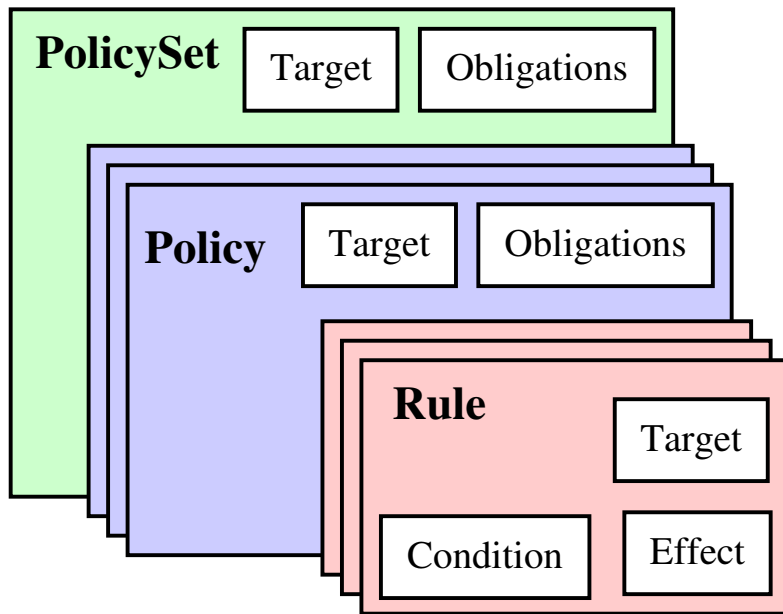
- ▶ New **subject** statements.
- ▶ Allows the specification of a full delegation chain.



eXtensible Access Control Markup Language



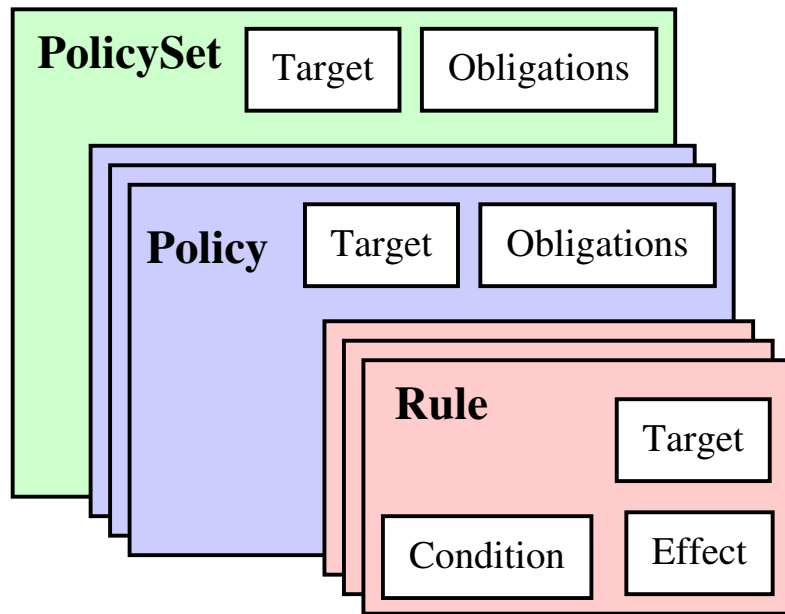
eXtensible Access Control Markup Language



► Target

- ▷ Subject
- ▷ Resource
- ▷ Action.

eXtensible Access Control Markup Language

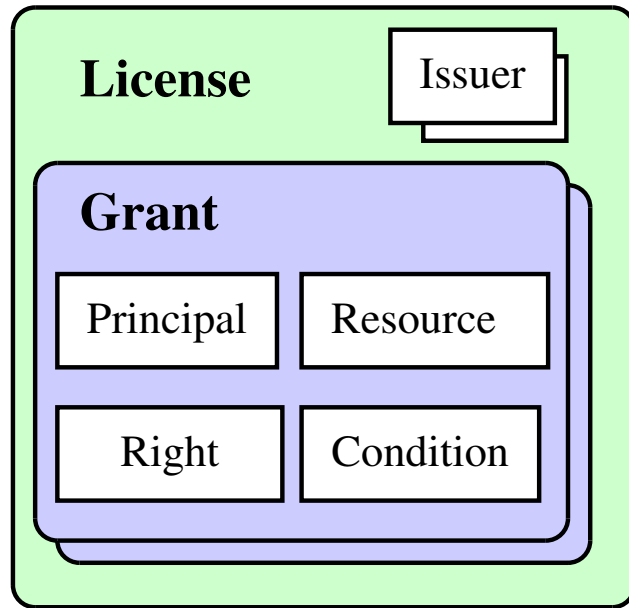


► Target

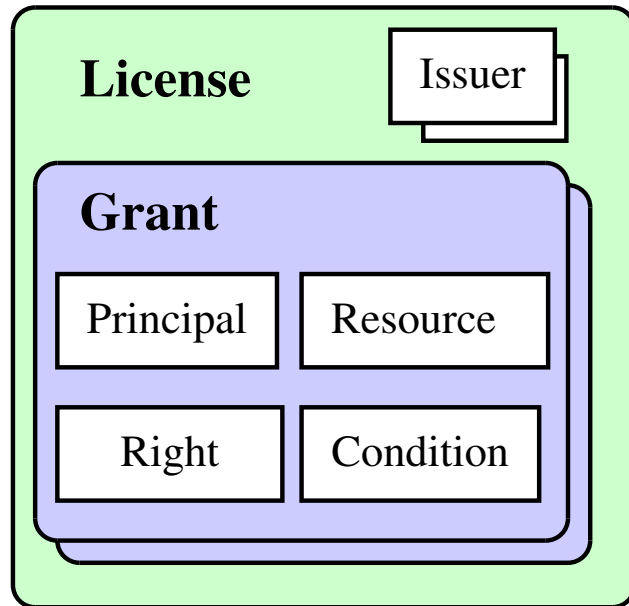
- ▷ Subject
- ▷ Resource
- ▷ Action.

- Consider **delegation as an *action***, the *resource* is the permission to delegate expressed as another *target*.
- Do not need to change the XACML specification.

eXtensible rights Markup Language (XrML)

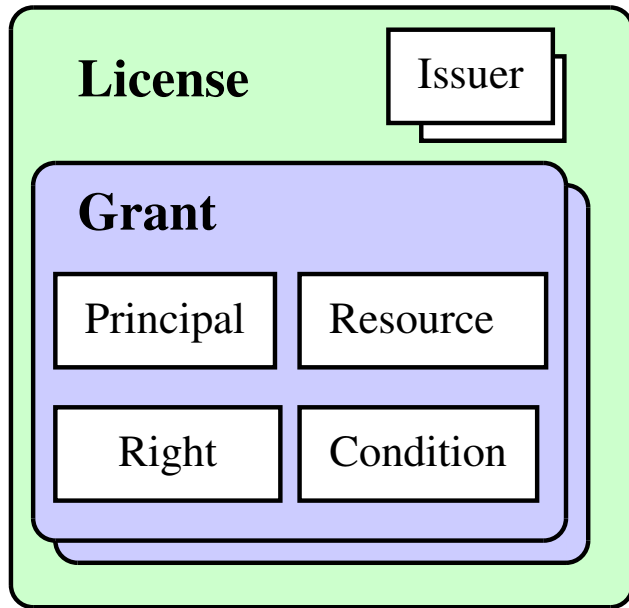


eXtensible rights Markup Language (XrML)



- ▶ Support for Delegation:
 - ▶ *DelegationControl*
 - ▶ Issue right

eXtensible rights Markup Language (XrML)



- ▶ Support for Delegation:
 - ▷ *DelegationControl*
 - ▷ Issue right

- ▶ By combining the **DelegationControl** and the **issue right** we can achieve constrained delegation.

Conclusions

- ▶ Constrained delegation provides valuable advantages to the distributed management of AC and DRM.
- ▶ Current XML-based standard should support it.
 - ▷ SAML: need to extend the specification.
 - ▷ XACML: somehow supported.
 - ▷ XrML: fully supported.

Constrained Delegation for XML-based Access Control and Digital Rights Management Standards

Guillermo Navarro, Babak Sadighi Firozabadi, Erik Rissanen, Joan Borrell

gnavarro@ccd.uab.es

Policy Based Reasoning Group,
Swedish Institute of Computer Science (SICS)

Combinatorics and Digital Communication Group
Universitat Autònoma de Barcelona.