# XACML Policy Profile for Multidomain Network Resource Provisioning and Supporting Authorisation Infrastructure

Yuri Demchenko, Mihai Cristea, Cees de Laat
System and Network Engineering Group,
University of Amsterdam
Amsterdam, The Netherlands
e-mail: {demch, cristea, delaat}@science.uva.nl

***Abstract*—Policy definition is an important component of the consistent authorisation service infrastructure that could be effectively integrated with the general resource provisioning workflow and network control and management plane. The paper describes the proposed XACML-NRP policy and attributes profile for Network Resource Provisioning. In addition to specifying a set of subject, resource, action attributes that are required for consistent XACML policy definition, the proposed profile allows also handling network path information what is especially important for QoS enforcement. To overcome stateless character of XACML policies, the proposed authorisation infrastructure provides a number of security mechanisms to support such important for NRP functionality as authorisation session and interdomain security context management, simple delegation, conditional authorisation decisions, and policy obligations handling.**

***Keywords - XACML; authorisation policy; authorisation session; Network Resource Provisioning (NRP); XACML-NRP.***

## I. INTRODUCTION

Authorisation infrastructure is a part of the modern high-performance network provisioning. With wider use of Grid and Cloud Computing that extensively use computing and storage resources virtualisation there will be increasing need for on-demand network infrastructure provisioning.

Security and authorisation services to support NRP should have high granularity, capable of dynamic invocation at different networking layers, support all stages of the provisioned resources lifecycle, and be capable of seamless integration with Grid and network middleware [1,2].

In this paper we summarise our recent developments and discuss in details the policy requirements and the proposed XACML-NRP policy profile that specifies a common set of attributes that are used in access control to networking services at all NRP stages. The paper develops further our research presented at the POLICY2007 workshop that reported our experience with using SAML and XACML for complex resource provisioining in Grid applications [3].

The proposed XACML-NRP profile is built upon and extends the XACML-Grid policy and attributes profile [4] developed as a cooperative effort between large international Grid projects and consortia with active authors' participation.

The paper is organised as follows. Section 2 refers to the NRP workflow to identify the key requirements to the authorisation policy and supporting authorisation infrastructure. Section 3 describes the XACML policy logical model and provides reference to few known XACML policy implementations. Section 4 proceeds with describing attributes used for access control policy definition in NRP. Sections 5 and 6 provide practical recommendations for attributes format definition and policy identification and resolution. Section 7 provides information about the XACML-NRP profile implementation in the GAAA Toolkit.

## II. NETWORK RESOURCE PROVISIONING MODEL AND AUTHORISATION POLICY REQUIREMENTS

The typical on-demand network resource provisioning process includes four major stages: (1) resource reservation; (2) deployment (or activation); (3) resource access/consumption; and additionally (4) resource de-commissioning after it was used [1].

The reservation stage may require the execution of complex procedures that may also request individual resources authorisation. At the deployment stage, the reserved resources are bound to a reservation ID, which we will refer to as the Global Reservation Identifier (GRI) that identifies the reserved resources.

In the discussed NRP model, domains are defined (as associations of entities) by a common policy or a single administration, with common namespaces and semantics, shared trust, etc. To ensure inter-domain policy and AuthZ services interoperability the NRP and AuthZ service/infrastructure should use common operational model, like defined by NRP, common logical model and common or mapped attributes semantics. In this case, the domain related security context may include:

- static security context such as domain based policy authority reference, trust anchors, all bound by the domain ID and/or domain trust anchor;
- dynamic or session security context bound to the GRI and optionally to a Local Reservation ID (LRI).

A policy framework and corresponding authorisation infrastructure to support NRP should meet the following requirements:

- Allow for multidomain access control policy definition and interdomain security context management, including cross-domain authorisation session management.

- Allow conditional AuthZ decision that should be evaluated in the next domain.
- Support topology based policy conditions and rules
- Support simple group or session based delegation with full or limited delegation profile.
- Use open standards and AuthZ mechanisms that could be easy integrated into the network services.

In particular, the last requirement indirectly implies limitation on separating context and state management between stateless policy definition and authorisation mechanisms to evaluate and manage inter-domains security context and conditional policy decision. In other words, policy should be stateless and security context and state management should be outsourced to a separate context handling functionality (in [1] it is defined as ContextHandler) that support communications between Policy Enforcement Point (PEP) and Policy Decision Point (PDP) intercepting actions related to state information and modifying if necessary.

## III. XACML Policy Logical Model and Implementations

Since development of the first XACML version in 2003 and releasing its Open Source reference implementation in the SunXACML Java library [5, 6], its appreciation is growing and more projects, applications and systems are using XACML for access control policy definition. In the current version the XACML framework is extended with the number of profiles, and in particular, with the SAML-XACML profile that allows XACML request-response messaging over the secure SAML2.0 protocol [7, 8] to support secure communication between remote XACML policy decision and policy enforcement points.

There is no much practically oriented papers and research that describe XACML policy use for real use cases, in particular for network resources. Two known implementations are G-PBox [9] and mentioned above XACML-Grid profile [4]. G-PBox is used for policy enforcement in Grid applications and allows also for hierarchical policy combination.

### A. XACML Policy Logical Model

A XACML policy is defined for the target tuple "Subject-Resource-Action-Environment" (S-R-A-E) which is also used for policy matching to the request.

```
Target (S, R, A, E) =>
       Target (M(Sreq, Spol), M(Rreq, Rpol),
               M(Areq, Apol), M(Ereq, Epol))
```

where M – is a matching function between attributes provided in the request and embedded in the policy.

It is important to mention that XACML allows only 2 variables matching functions in the Target element which however can be cascaded [5].

XACML policy can contain a number of rules which in its own turn may contain a number of conditions and a rule Target used for rules matching (or selection). The Conditions can use a wide range of functions defined in the XACML specification [5]. The following describes the structure of the Rule element:

```
Rule(Target (S, R, A, E),
     Condition (F(Sreq, Spol), F(Rreq, Rpol),
                F(Areq, Apol), F(Ereq, Epol)),
     Obligations)
```

where F – is a logical function with attributes provided in the request and embedded in the policy.

Additional flexibility for XACML policy rules definition is provided by the possibility to use the full functionality of the XPath expressions to select any of elements or attributes in the XACML Request message which is referred to as "xacml-context". This functionality is used in the proposed XACML-NRP profile for defining rule conditions based on the provided network topology description.

The XACML policy can also specify the Obligations as actions that must be taken on positive or negative authorisation decisions. Introducing policy obligations allows for more flexible policy definition by separating stateless conditions that are based on the information provided in the access control request and stateful conditions that may depend on the target system/resource state.

## IV. Attributes Used for Authorisation and XACML Policy Definition

### A. Network or resource related attributes

Network related attributes allow building policy depending on the network topology or other network characteristics.

Topology format should provide necessary information about the network resource to allow consistent policy evaluation, and vise versa the policy format may be defined by the network topology to which the policy is applied. Initial set of the XACML-NRP topology related attributes was derived from the currently being developed Network Description Language (NDL) [10] and Network Mark-up Language (NML) [11]

Network related attributes are considered as a part of the XACML Resource definition. The following resource/network related attributes can be specified and used for authorisation:

- Domain (network domain)
- VLAN, Transport Network Address (TNA)
- Interface ID, Link ID, Device or resource-type
- Link parameters: average delay and maximum bandwidth
- ReservationEPR that may directly or indirectly define the resource federation or administrative domain
- Federation that defines a number of domains or nodes sharing common policy and attributes

### B. Subject related attributes

Subject related attributes allow building policy depending on the properties of the request Subject or user. The following subject related attributes can be specified:

- Subject ID
- Subject confirmation that contains AuthN assertion/token or other attribute confirming subject's ID by trusted AuthN authority

- Subject Role and/or Group
- Subject Federation (e.g., Virtual Organisation, etc.)
- Subject context that can provide additional information about the Subject other than Subject federation e.g. such as Session ID, or project/experiment name

Typically Subject attributes are provided as Subject credentials which depending on user client implementation and middleware may take a form of X.509 public key and attribute certificates (PKC, AC), SAML Authentication and Attribute assertions, proprietary AuthN system credentials.

### C. Action and Environment related attributes

Action related attributes represent a limited number of the specific actions that requesting party can ask to initiate network resource reservation, access or management.

Environment related attributes allow providing additional information for policy definition and evaluation. There is no specific Environment attributes identified for the XACML-NRP profile but this may be a place to put security context related information from the previous domain.

### D. Policy Obligations used in NRP

Policy obligation is one of the authorisation policy enforcement mechanisms that allows adding AuthZ decision enforcement components that can not be defined in the policy at the moment of making policy decision by the PDP, or may not be known to the policy administrator.

Suggested functionality that can be achieved with using obligations includes but not limited to:

- Intra-domain network/VLAN mapping for cross-domain connections, that can be used to map external/interdomain border links/TNA's to internal VLAN and sub-network
- Network identity and account mapping
- Type of service (or QoS) assigned to a specific request or policy decision
- Service combination with implied conditions (e.g., computing and storage resources)
- Usable resources/quota

Refer to [12] for the proposed by authors the obligations handling model.

## V. Attributes Expression Conventions

One of important components to ensure AuthZ policy interoperability is defining rules and conventions for attributes expression. Below we provide suggestions and examples for the Resource and Subject attributes expression. The Action attributes can use either simple string format or enumerated URN or URL style similar to the Resource attributes. Although the proposed description is based on the current XACML-NRP and GAAA-TK library implementation in the Phosphorus project [13], authors believe that this information will be useful for researchers and developers working in this area.

### A. Resource attributes

In current implementation the Resource variable in the AuthZ request contains one attribute ResourceURI in the form of URI string that includes the network resource identifier and a list of parameter used for policy-based request evaluation. When sending a XACML Request to XACML PDP the input URI string is converted into the set of the Resource attributes (organised as a HashMap). The attribute names are taken from the XACML-NRP profile, such as "resource-id", "resource-domain", "resource-realm", "resource-type", "source", "target", etc.

The following ResourceURI formats are supported:

```
a) http://testbed.ist-phosphorus.eu/{domain}/
   {device | service}/{parameters}
```

For example, the following URI will be converted to the set of resource attributes

```
http://testbed.ist-phosphorus.eu/viola/
    harmony/source=10.7.12.2/target=10.3.17.3
resource-id =
    http://testbed.ist-phosphorus.eu/viola/harmony
resource-realm = http://testbed.ist-phosphorus.eu
resource-domain = viola
resource-type = harmony
source = 10.7.12.2; target = 10.3.17.3
b) http://testbed.ist-phosphorus.eu/
       resource-type/{resource-type-name}
```

### B. Subject attributes

The Subject variable of the AuthZ request may contain the following attributes:

a) SubjectId (attribute identifier "subject-id") – subject identifier in RFC822 (email) or X.521 (LDAP or X.509 Public Key Certificate) formats

Example: `WHO740@users.testbed.ist-phosphorus.eu`

b) SubjectConfirmatioData (attribute identifier "subject-confdata") – Authentication assertion or token provided by the trusted AuthN service (can be also SAML AuthN Assertion, X.509 or VOMS attribute certificate), or crypto-string provided local AuthN service.

c) SubjectRole (attribute identifier "subject-role")

Example: `admin, or researcher@project01, or admin@viola.testbed.ist-phosphorus.eu`

d) SubjectContext (attribute identifier "subject-context") - this attribute is used for providing additional information about a user association like VO, project, experiment/job.

Example: `demo001; or VO-Phosphorus`

## VI. Policy Identification and Policy Resolution

When evaluating AuthZ request the ContextHandler or PDP (refer to [1, 13] for the generic AuthZ service architecture and basic AuthZ service components participating in AuthZ process) need to find/select an applicable policy. This is typically done based on the request parameters such as Resource or Subject attributes.

The policy selection comprises of two steps: policy resolution and policy retrieval. Policy resolution means extracting such information from the AuthZ request that can be used for further policy selection in the storage/repository. Based on this information, a repository request or query can be constructed to retrieve proper policy.

Note, it is a SunXACML implementation convention that only one Policy or PolicySet should be supplied to PDP for evaluation, and only one component Policy must be selected if using PolicySet.

The following components of the XACML-NRP profile can be used for policy resolution:

a) resource ID and resource attributes;

b) subject attributes defining context in which the request should evaluated, e.g. federation, VO or project (this information is typically a part of the subject attributes);

c) attributes and policy profile namespace, which can actually be a part of the resource ID if expressed in Fully Qualified Attribute Name format (FQAN format).

Depending on the policy storage/repository implementation, the following components can be used for policy identification:

a) file name and directory, if policy is stored as a file;

b) PolicyId attribute of the PolicySet or Policy element;

c) policy Target element that can include any of Subject, Resource, Action, Environment elements.

Although using basically different ways of storing policies, the first case and second identification methods can be based on similar approach to composing PolicyId attribute and defining policy file location path. When using third option, the policy repository should be capable to query policy database by the policy Target content.

## VII. XACML-NRP Profile Implementation in the GAAA-Toolkit Library

All required functionality to support GAAA-NRP authorisation infrastructure is currently being implemented in the GAAA Toolkit (GAAA-TK) pluggable Java library in the framework of the Phosphorus project [13]. The library allows for AuthZ request evaluation with the local XACML based PDP or calling out to the external AuthZ service using the SAML-XACML protocol.

XACML-NRP profile is implemented as a configurable metadata set that defines the supported attributes semantics, expression format and resolution methods like described above.

One of the key functional components to support AuthZ session management using AuthZ tokens as session credentials is the Token Validation Service (TVS). It is implemented as a part of the general GAAA-TK library but can also be used separately and integrated into other AuthZ frameworks.

The GAAA-TK library provides few PEP and TVS methods that support extended AuthZ session management and provide necessary AuthZ tokens and tickets handling functionality (refer to the GAAA-TK release documentation [13] for the complete API description).

## VIII. Summary and Future Development

This paper presents the results of the ongoing research and development of the generic AAA AuthZ architecture in application to on-demand optical network resource provisioning. It is based on the real implementation of the proposed XACML-NRP policy and attributes profile in the Phosphorus project and summarises experiences gained from this practical work.

The proposed XACML-NRP profile is implemented in the pluggable GAAA-TK library as a configurable metadata set that defines the supported attributes semantics, expression format and resolution methods. The current implementation will provides a good basis for further research on improving efficiency of the proposed solutions.

Further development of the proposed XACML-NRP policy and attributes profile will require wider Grid and networking community discussion to define basic set of network and user related attributes that should allow flexible definition of the topology aware XACML policies and easier integration with Grid applications.

## References


[1] Demchenko Y, A. Wan, M. Cristea, C. de Laat, “Authorisation Infrastructure for On-Demand Network Resource Provisioning,” Proc. The 9th IEEE/ACM Int. Conf. on Grid Computing (Grid 2008), Tsukuba, Japan, Sept. 29 - Oct. 1, 2008. Pp. 95-103. IEEE Catalog Number CFP08GRI-CDR, ISBN 978-1-4244-2579-2.

[2] Phosphorus Project. [Online]. Available at: http://www.ist-phosphorus.eu/

[3] Demchenko, Y.; Gommans, L.; de Laat, C., "Using SAML and XACML for Complex Resource Provisioning in Grid Based Applications," Proc. International Workshop on Policies for Distributed Systems and Networks, 2007 (POLICY2007). Bologna, Italy, 13-15 June 2007. ISBN-13: 978-0-7695-2767-3, ISBN-10: 0-7695-2767-1. pp. 183-187.

[4] “An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids,” Joint EGEE, OSG, and Globus document. [Online]. https://edms.cern.ch/document/929867/1

[5] "eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005.” [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_ control-xacml-2.0-core-spec-os.pdf

[6] SunXACML Java library. [Online] Available: http://sunxacml.sourceforge.net/

[7] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[8] “SAML 2.0 Profile of XACML 2.0, Version 2. Working Draft 2, 26 June 2006”. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/xacml-2.0-profile-saml2.0-v2.zip

[9] Cesini, D., V. Ciaschini, D. Dongiovanni, A. Ferraro, A. Forti, A. Ghiselli, A. Italiano, D. Salomoni, “Enabling a priority-based fair share in the EGEE infrastructure”, Proc. Int. Conf. Computing in High Energy and Nuclear Physics (CHEP’07), IOP Publishing, Journal of Physics: Conference Series 119 (2008)

[10] Ham, J, van der, et al:,”Using the Network Description Language in Optical Networks,” Proc. 10th IFIP/IEEE Symposium on Integrated Network Management , May, 2007

[11] Open Grid Forum Network Mark-up Language Working Group (NML-WG). [Online] https://forge.gridforum.org/sf/projects/nml-wg

[12] Demchenko, Y., C. de Laat, O. Koeroo, H. Sagehaug, “Extending XACML Authorisation Model to Support Policy Obligations Handling in Distributed Applications,” Proc. The 6th International Workshop on Middleware for Grid Computing (MGC 2008), December 1, 2008, Leuven, Belgium. ISBN:978-1-60558-365-5.

[13] “GAAA Toolkit pluggable components and XACML policy profile for ONRP", Phosphorus Project Deliverable D4.3.1. – September 30, 2008. [Online]. Available: http://www.ist-phosphorus.eu/files/deliverables/Phosphorus-deliverable-D4.3.1.pdf

[14] RFC 2904 - "AAA Authorization Framework" J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, August 2000 - ftp://ftp.isi.edu/in-notes/rfc2904.txt