



Project no. 032691

# KnowARC

***Grid-enabled Know-how Sharing Technology Based on ARC Services and Open Standards***

*Specific Targeted Research Project*
*Information Society Technologies*

# D1.6-2 INTEGRATION OF A DELEGATION POLICY ENGINE AND POLICY PARSER INTO KNOWARC

---

***Due date of deliverable:*** June 2, 2008 ***Actual submission date:*** June 9, 2008

***Start date of project:*** June 1, 2006 ***Duration:*** 39 months

***Organisation name of lead contractor:*** NG-UiO

***Revision:*** 1.0

| **Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)** | | |
|---|---|---|
| **Dissemination Level** | | |
| **PU** | Public | X |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |
| **CO** | Confidential, only for members of the consortium (including the Commission Services) | |

# Contents

# 1 Introduction

This is the second deliverable of Task 1.6, *Security Framework*. While the first deliverable, D1.6-1 – *KnowARC security review*, aims at evaluating ARC1 components including the interfaces from Task 1.2, Task 1.3 and Task 1.4, as well as higher level services and clients of WP2, and providing an early feedback for the development tasks; this deliverable aims at implementing a policy parsing and evaluation infrastructure, as well as implementing an enhanced identity delegation solution by utilizing policy evaluation engine.

This deliverable presents implementation of policy evaluation engine and fine-grained policy constraints mechanism for identity delegation. The current implementation includes ARC policy evaluation engine which can consume the policy and request in ARC specific schema, and delegation constraints solution using policy evaluation engine and RFC3820 proxy certificate specifications.

This deliverable consists of this *deliverable report*, the *code* and the related *technical documentation*. It is currently available in 0.9 development branch (hereafter mentioned as ARC1) of ARC middleware and will be available in the production release version 1.0.

# 2 Purpose and Content

The X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile (RFC3820) defines widely-used standard for identity delegation and single sign on in Grid community. However current usage practices have some deficiencies. Commonly only two mechanisms are used for limiting capabilities of generating credentials. Those are limiting depth of delegation and adding time constraints to proxy certificates. Usually no other restrictions are defined, which makes the delegation uncontrollable and unpredictable in a Grid world made of chains of multiple services.

To restrict possible misuse of delegated credentials by untrusted intermediate services some kind of fine-grained delegation mechanism is needed.

The current implementation contains the following aspects:

- *ARC security framework:* ARC1 middleware is based on service container framework called Hosting Environment Daemon (HED) (D1.2-2[1]) which contains an interface for implementing and enforcing authentication and authorization. This interface is functional in some plug-ins called SecHandler. The SecHandler is pluggable and can be configured by using configuration file. Under the SecHandler there could be some pluggable and configurable sub-modules which specifically handle various security functionalities, such as authorization, authentication, etc.
- *ARC policy schema and policy evaluation engine:* ARC1 defines specific evaluation request and policy schema. Based on the schema, one policy evaluation engine is implemented for parsing the policy, and evaluating the request against policy. The design principal of policy evaluation engine is

[1] The ARC container (first prototype). https://www.knowarc.eu/documents/Knowarc_D1.2-2_07.pdf

generality by which the implementation of the policy evaluation engine can be easily extended to adopt some other policy schema, such as XACML policy schema[2].

- *Using ARC policy evaluation engine for fine-grained identity delegation:* ARC delegation PDP (policy decision point) is implemented for matching security attributes (such as identity of client, requested action, targeted resource) to delegation policy by invoking the policy evaluation engine. The delegation policy is inserted in the X509 proxy certificate (RFC 3820) by client, extracted by TLS level message component on service side, and evaluated by delegation PDP which is configured on service side.

# 3 Code and Documentation

A tarball of the source code is available from the web page of the KnowARC project [3] . Basic functionality of policy evaluation engine is located in src/hed/libs/security folder. Its implementation for ARC specific policy along with other pluggable security related components may be found under src/hed/pdc. Some other code performing collection of information used in making authorization decisions resides inside Message Chain Components plugins under src/hed/mcc. Credentials delegation interface and utility are placed into src/hed/libs/delegation and src/clients/credentials correspondingly.

Since the security related code uses a lot of common functionality of hosting environment daemon infrastructure, and it is also used by the other parts here and there, it can't be easily separated from rest of ARC source tree. The code in the tarball is just a snapshot of the source code related to this deliverable, and is only for code viewing, not for compiling. If it is needed to test the functionality, please download the code from ARC1 svn[4] and compile it.

The code is developed using the C++ programming language, and the dependent third-party libraries are the same as those in D1.2-2.

The technical documentation corresponding to this deliverable is available in the form of a NorduGrid technical documentation[5].

# 4 Conclusion and Future Work

The deliverable provides a general and extensible policy evaluation engine. Based on the policy evaluation engine, an identity delegation constraining solution is provided for fine-grained delegation.

Some standard policy schema could need to be supported for interoperability. The candidate is XACML which is a widely accepted policy schema.

---

[2] XACML policy schema. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd

[3] http://www.knowarc.eu/download/D1.6-2_08_code.tgz

[4] http://svn.nordugrid.org/repos/nordugrid/arc1/trunk/

[5] Aleksandr Konstantinov, Weizhong Qiang, *Security Infrastructure of ARC1*, http://www.knowarc.eu/download/D1.6-2_08_documentation.pdf

Currently, for the policy exchanging in delegation scenario, the textual representation of ARC Policy XML document is inserted into ProxyPolicy extension of proxy certificate, and the integrity of policy is guaranteed by the certificate signature. For the policy exchanging in some general scenario, some other solution could be provided to guarantee the integrity of policy, for instance, "SAML profile of XACML 2.0[6]" can be implemented to provide integrity for XACML policy.

[6] http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf