Support for Authentication Profiles in Argus

Andrea Ceccanti

1 Introduction

We need a flexible mechanism for expressing Authentication profiles, aka CA Levels of Assurance (LoA) in Argus. At the moment the extension still only entails allowing CAs classified as DOGWOOD, the Identifier-Only Trust Assurance (IOTA) profile, as an additional permitted authentication source in combination with selected (VO) attribute authorities. But in the near future, there will be more new LoAs that will need to be supported. Within the EGI and related ecosystems, this will include the assurance profiles coming from the REFEDS Assurance WG (specifically the proposed combined assurance clusters Cappuccino and Espresso) as well as the EGI CheckIn assurance profiles that are scoped to the service providers within EGI.
To support different CA LoAs, we propose to introduce support for the VO-CA-AP file, which describes which LoAs are allowed for which VOs (and which LoAs for certificates without VOMS extensions). The advantage of this approach is that it is backward compatible (existing policies continue to work as expected) and requires no special monitoring or deployment procedure to ensure that new LoAs are not enabled by mistake on all resources or for all VOs.
The disadvantage of this approach is that the LoAs are not visible and cannot be used to write policies. If an LoA is enabled for a VO, it is enabled for all resources in that VO. However, this limitation can be avoided by implementing an additional PIP that takes care of providing information about the LoA in form of request attributes (and we already have two proposals on how to do that).
In practice, we propose to introduce a new Policy Information Point that can parse the VO-CA-AP file and can set certificate-related attributes (subject, subject-issuer, vo, fqan, etc…) if the LoA of the certificate linked to the authorization request is allowed by the VO-CA-AP configuration.

2 Problem description

A problem with the introduction of differentiated LoA is that in the EGI and WLCG infrastructure, until now, all CAs were either allowed or not. Hence a VO is automatically allowed to use any CA LoA, also the ones that are not yet in existence and ones that are of a lower LoA than the currently existing ones. We need to ensure that new LoAs are only supported on resources as a result of an administrator adding a policy in Argus that enables such support.

3 Requirements

A number of requirements for a flexible and future-proof solution can be recognized:

1. It should be possible to enable/disable CA LoA for a given supported VO
2. CA LoA support should have minimal performance impact

3. It should be possible to define complicated policies matching combined LoAs, e.g. to enable DOGWOOD only for a given FQAN or a given set of resources
4. A VO must NOT automatically become eligible for all LoAs when new assurance profiles are enabled on the infrastructure.

4 Suggested solution

We propose to define an additional PIP, running in the Argus PEP daemon/PDP, that has the responsibility of understanding the LoA of the user certificate in the authorization request and choose, if such LoA is allowed by a local policy file (not to be confused with Argus policies stored in the PAP), populate the request with the certificate-related attributes (i.e., subject, subject-issuer, vo, fqan and pfqan and EMI profile equivalents). If the LoA is not allowed by the policy, relevant attributes are removed from the request (which will then result in a NotApplicable authorization decision).

We will use the VO-CA-AP policy syntax to define which LoAs are allowed for which VOs and for certificates without VOMS extensions.

Requirement	Solution
It should be possible to enable/disable CA LoA for a given supported VO	in order to enable an LoA for a given VO an entry must be present in the VO-CA-AP file that allows such LoA for such VO. To disable the LoA for a VO, the entry in the VO-CA-AP file must be changed to not include such LoA.
CA LoA support should have minimal performance impact	no significant performance impact is expected.
It should be possible to define complicated policies matching combined LoAs, e.g. to enable DOGWOOD only for given a FQAN on given set of resources	By exposing the authentication profile of the current certificate in the request, it is also possible to define policies that are applied after the check implemented by the authentication profile PIP. This gives the possibility of having policies that allow/deny an authentication profile (allowed by the VO-CA-AP file) only on specific resources/actions.
A VO must not automatically become eligible for all LoAs when new assurance profiles are enabled on the infrastructure.	This requirement is solved naturally by this proposal. No migration strategy or monitoring strategy has to be put in place. The only thing sites have to do is to upgrade to the Argus version that

	implements this proposal and install the VO-CA-AP RPM.

4.1 External checks

No external checks are needed to ensure that new LoAs are enabled by mistake with this proposal.

5 Implementation

5.1 Description of the changes to existing code

The VO-CA-AP parsing logic is developed in a way that supports reloading the file contents periodically without requiring service restarts.

A new PIP is introduced which is run after the GLITE Authorization Profile PIP and CommonXACMLProfile PIP, that enforces the LoA checks described in section 4, the attributes subject, issuer, vo, fqan, pfqan (and similar attributes in the CommonXACML profile) are only issued if the certificate linked to the authorization request satisfies the policies defined in the VO-CA-AP configuration.

5.2 Estimated effort required for the changes

1 FTE week of development/testing work.

6 Operation

6.1 Upgrade procedure from 1.7.0

The upgrade procedure from 1.7.0 is as follows:

- Install Argus 1.7.1 RPMs
- Reconfigure the PEPd service to ensure the new LoA-aware PIP is used by the PEPd configuration
- Install EGI dogwood CAs RPM
- Install RPM that provides the VO-CA-AP file (or write your own file)
- Restart the services

6.2 Procedure to enable/disable support for a LoA for a VO

As already introduced in section 4, in order to enable an LoA for a given VO the VO-CA-AP file must have an entry that enables such LoA for that VO. To disable the LoA for a VO, the entry in the VO-CA-AP file must be changed to not include such LoA.