# Introducing support for CA Level Of Assurance in Argus

Andrea Ceccanti

# 1 Introduction

We need a flexible mechanism for expressing CA Levels of Assurance (LoA) in Argus policies. 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 ecosystem, this will include the assurance profiles coming from the REFEDS Assurance WG (specifically the proposed combined assurance clusters Capuccino 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 new attributes for each new LoA (or group of related LoAs), so that each LoA, in order to be authorized (or denied) for a given resource, needs to be explicitly included in a policy. The advantage of this approach is that is backward compatible (existing policies continue to work as expected) and requires no special monitoring or deployment procedure to ensure that new LoAs are enabled by mistake on all resources or for all VOs.
In practice, we propose to introduce a new Policy Information Point that can map LoA linked to a certificate to a certain attribute that can be later used to write policies targeting such LoA. This mapping is configurable, so that you can have a one-to-one mapping between LoA and attribute or create a mapping that will map multiple LoAs to a single attribute, if this approach is convenient for your deployment.

# 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 given a FQAN, e.g. Role=VO-Admin, on 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 a new set of attributes targeting each new LoA (or group of related LoAs) introduced in the infrastructure, by extending the profile Argus uses to enforce XACML policies.
Currently we have the following attributes, used in our infrastructure, that are used to write policies targeting certificates (and VOMS attribute certificates):

- **subject, subject-issuer, vo, fqan, pfqan**

In order to ensure that the meaning of these attributes in the profile currently used in production doesn't change, we propose to change Argus so that these attributes are only assigned to certificates linked to the LoAs currently used in production (i.e. aspen, birch and cedar, according to the terminology defined here).
To target the new dogwood LoA, we propose to introduce an additional set of attributes

- **iota-subject, iota-subject-issuer, iota-vo, iota-fqan, iota-pfqan**

These attributes have similar behaviour to the ones described above but will only match certificates and VOMS attribute certificates linked to certificates issued by CAs of LoA dogwood.
Whenever a new LoA is introduced, we propose to introduce an additional set of attributes for such LoA (or group of related LoAs), as it is done for dogwood above. So for instance, for the elm LoA, which IIRC will be introduced sometime in the future, and linked to certs obtained after a multi-factor authentication check, we propose to introduce the following attributes:

- **mfa-subject, mfa-subject-issuer, mfa-vo, mfa-fqan, mfa-pfqan**

We don't expect to have more than 5-6 types of different LoAs for CAs in IGTF, so this approach is manageable.
The requirements in section 3 are satisfied as follows:

| 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 a policy rule with the proper attribute for such LoA (vo,fqan, or pfqan) has to be defined. To disable the LoA for a VO, the rules containing LoA attributes targeting such VO must be removed. |
| CA LoA support should have minimal performance impact | no significant performance impact is expected. Checking that a policy matches will mean for the PDP checking the presence of a single attribute and, if present, comparing its value against the |

| | |
|---|---|
| | target vo/fqan/pfqan value. For resources that will support multiple LoAs more rules will have to be evaluated, but I don't expect significant overhead from this. |
| 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 | Combining different LoAs for a resource/action means adding rules for such LoAs for a given resource. Having different set of attributes for each LoA (or group of related LoAs) allows to have all the flexibility needed to write complex policies. See the examples section below. |
| 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. |

## 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

A new PIP is introduced, based on the GLITE Authorization Profile PIP and supporting the same profile IDs, which enforces the LoA checks described in section 4, and in particular that:

- the attributes subject, issuer, vo, fqan, pfqan are only issued to certificates issued by CAs in LoA aspen, birch, cedar.
- the attributes iota-subject, iota-issuer, iota-vo, iota-fqan, iota-pfqan are only issued to certificates issued by CAs in LoA dogwood.

This PIP can be implemented to accomodate configurable LoAs mappings to attributes, so that new LoAs do not require changes to code, but only to configuration.
The code that allows to determine the LoA for a given certificate is derived from what is already available in this pull request.
The PAP attribute mappings INI file is changed to add the additional attributes.

## 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
- Restart the services

In order to enable dogwood LoAs for eligible VOs, new policies using the new iota attributes will have to be added to the existing policies. This procedure can be automated by introducing small changes to the logic in this script so that new rules are added for VOs that are iota-enabled.

### 6.1.1 Examples

Assuming the policy configuration is as follows:

```
resource "cms-1" {
   action ".*" {
      rule permit { vo="cms" }
   }
}

resource "cms-analysis" {
   action ".*" {
      rule permit { pfqan="/cms/analysis" }
   }
}

resource "cms-production" {
   action ".*" {
      rule permit { pfqan="/cms/production" }
   }
}

resource "dteam" {
   action ".*" {
      rule permit { vo="dteam" }
```

```
    }
}
```

in order to enable iota support for CMS,  the resulting policy would become:

```
resource "cms-1" {
    action ".*" {
        rule permit { vo="cms" }
        rule permit { iota-vo="cms" }
    }
}

resource "cms-analysis" {
    action ".*" {
        rule permit { pfqan="/cms/analysis" }
        rule permit { iota-pfqan="/cms/analysis" }
    }
}

resource "cms-production" {
    action ".*" {
        rule permit { pfqan="/cms/production" }
        rule permit { iota-pfqan="/cms/production" }
    }
}

resource "dteam" {
    action ".*" {
        rule permit { vo="dteam" }
    }
}
```

## 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 a policy rule with the proper attribute for such LoA (vo, fqan, or pfqan) has to be defined. To disable the LoA for a VO, the rules containing LoA attributes targeting such VO must be removed.

### 6.2.1 Examples

See section 6.1.1 for an example of enabling dogwood LoA for VO CMS. The disabling operation is the inverse, i.e. removing all rules containing iota- attributes for that VO.