

AA-RR

Current Status

4th TF-AACE Meeting
6 June 2004

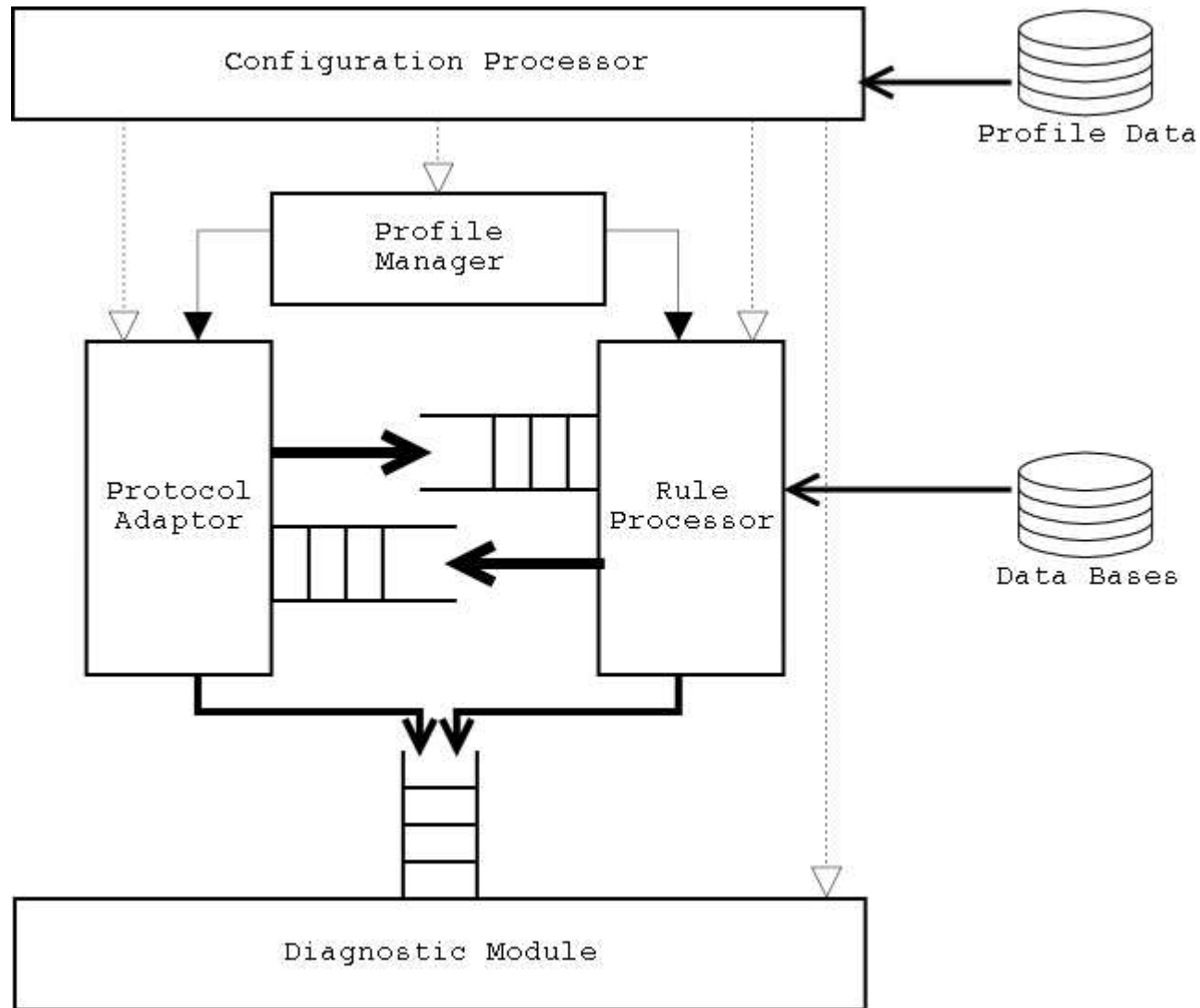


Red IRIS



- **Able to impersonate any of the following components**
 - Attribute sources (AS): Able to accept queries and respond with attribute information
 - Attribute requesters (AR): Make requests to AS and process them, possibly using AE
 - Authorization engines (AE): Responds queries from AR applying their internal rules
- **Driven by profiles**
 - Entity and protocol aspects
 - Attributes and values
- **Protocol agnostic**
 - SAML (and XACML)
 - SPOCP
 - RADIUS

- **A first prototype has been built**
 - Based on openSAML
 - Demonstrates the feasibility of the approach
 - Ideas for defining profiles
- **The other alternative protocols have been analyzed**
 - Common characteristics of AA interactions
 - Applicability of the approach of the initial prototype
- **A design of the system has been produced**
 - Modular
 - Extensible
 - Includes the mechanisms for defining profiles



- **Configuration Processor**
 - Reads profile data and instantiates the required components
- **Profile Manager**
 - Controls the execution of the different elements in the profile
- **Rule Processor**
 - Applies the rules defined to specify the behaviour of the AA-RR
- **Diagnostic Module**
 - Logs information about interactions and their results
- **Protocol Adaptor(s)**
 - Provides an uniform interface to the different protocol bindings
- **Profile Definitions**
 - Use a XML-based syntax
- **Data Bases**
 - Enable re-use of data in different experiments

```
<aardef binding="saml">
  <environment>
    <instance type="source"/>
    <workingdir path="/usr/local/aarr"/>
    <log level="28" output="saml/source-AQ-EPER.log"/>
    <base name="attNames" path="saml/attributeNames"/>
    <base name="attValues" path="attributeValues"/>
  </environment>
  <protocol>
    <listen at="http://aarr.rediris.es/demourl"/>
    <connect to="https://aatresp.edufederation.org"/>
    <keystore path="/usr/local/aarr/keystore"/>,
  </protocol>
  <run>
    <ruleset name="SAML AQ-eduPersonEntitlement-role"
      path="saml/AQ-EPER.ars"/>
  </run>
</aardef>
```

```
<ruleset name="SAMLAQ-eduPersonEntitlement-role">
  <state name="init">
    <rule name="i1">
      <conditions>
        <condition name="c1" receive="SAMLAttributeQuery"/>
        <condition name="c2" field="Attribute" value="eduPersonEntitlement"/>
        <condition name="c3" field="Attribute" base="attNames" key="roleAttr"/>
      </conditions>
      <actions>
        <action name="a1" send="SAMLAttributeResponse">
          <field id="AttributeValue" value="urn:mace:rediris.es:PAPIResources"/>
          <field id="AttributeValue" base="attValues" key="roleAttr"/>
        </action>
        <action name="a2" next="accepted"/>
      </actions>
    </rule>
    <rule name="idef">
      <conditions>
        <condition name="ca1" default="any"/>
      </conditions>
      <actions>
        <action name="ff" finish="fail"/>
      </actions>
    </rule>
  </state>
  .
  .
  .
```